



LYNX L-510



Web Interface User's Guide

ADSL2/2+ Access Point, Ethernet & USB Combo Router

Version 1.1

Table of Contents

Chapter 1	Declaration Of Conformity	4
Chapter 2	About this Manual	7
2.1	Introduction.....	7
2.2	Scope and Purpose	7
2.3	Targeted Audience.....	7
2.4	Manual Organization	7
Chapter 3	ADSL Ethernet Router Description	8
3.1	Features.....	8
3.2	Lynx L-510 Overview.....	10
Chapter 4	Your Gateway At A Glance.....	11
4.1	Ports and Buttons	11
4.2	Lynx L-510 Overview.....	12
Chapter 5	Installing The Lynx L- 510.....	14
Chapter 6	Setting Up the Lynx L-510	15
6.1	Logging into your Lynx L-510	15
6.2	Basic.....	16
6.2.1	LAN / DHCP Configuration	17
6.2.2	Diagnostic Test.....	19
6.2.3	Ping Test	20
6.2.4	Modem Test	20
6.3	Advanced	21
6.3.1	WAN Connection	22
6.3.2	New Connection	22
6.3.3	ADSL Modulation	22
6.3.4	Quickstart.....	23
6.3.5	LAN Configuration (VLAN)	25
6.3.6	LAN Clients.....	28
6.3.7	Ethernet Switch Configuration	28
6.3.8	Application (UPnP)	29
6.3.9	SNTP	30
6.3.10	SNMP	31
6.3.11	IP QoS.....	32
6.3.12	IGMP Multicast.....	33
6.3.13	Dynamic DNS Client	34
6.3.14	DNS Proxy	35
6.3.15	Easy Connect Configuration.....	35
6.3.16	Port Forwarding.....	36
6.3.17	MAC Filtering (Bridge Filters)	38
6.3.18	Access Control	38
6.3.19	Routing (Static Routing)	39
6.3.20	Dynamic Routing	40

6.3.21	System Password	41
6.3.22	Firmware Upgrade	42
6.3.23	Restore to Default	42
6.4	Wireless.....	43
6.4.1	Wireless Setup.....	43
6.4.2	Wireless Configuration	44
6.4.3	Wireless Security	44
6.4.4	Wireless Management	47
6.5	Security	48
6.5.1	IP Filters.....	48
6.5.2	LAN Isolation.....	49
6.6	Status.....	50
6.6.1	Connection Status.....	50
6.6.2	System Log.....	51
6.6.3	Remote Log Settings.....	52
6.6.4	Network Statistics	52
6.6.5	DHCP Clients	53
6.6.6	Modem Status.....	53
6.6.7	Product Information	54
6.7	Help.....	54
Appendix A: Troubleshooting		55
The Lynx L-510 is not functional.....		55
I can't connect to the Lynx L-510		55
The DSL Link LED continues to blink but does not go solid		56
The DSL Link LED is always off.....		56
APPENDIX B: Lynx L-510 terms		57
What is a firewall?.....		57
What is NAT?.....		57
What is a DMZ?.....		57
What is a Gateway?.....		58

Chapter 1 Declaration Of Conformity

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN300 328, EN301 489-17, EN60950

Countries of Operation and Conditions of Use in the European Community

This device is intended to be operated in all countries of the European Community. Requirement is for indoors vs. outdoors operation, license requirements and allowed channels of operation apply in some countries as described in this document.



Note: The user must use the configuration utility provided with this product to check the current channel of operation and confirm that the devices operating in conformance with the spectrum usage rules for the European Community countries as described below.

If operation is occurring outside of the allowable channels as indicated in this guide, then the user must cease operating the product and consult with the local technical support staff responsible for the wireless network.

This device may be operated indoors or outdoors in all countries of the European Community using the 2.4GHz band: Channels 1 – 13, except where noted below:

- In Italy the end-user must apply for a license from the national spectrum authority to operate this device outdoors.
- In France outdoor operation is only permitted using the 2.4 – 2.454 GHz band: Channels 1 – 7.

Radio Frequency Interference Warnings & Instructions

(FCC ID: I38-DSL600EWR)

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and the receiver
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected
- Consult the dealer or an experienced radio/TV technician for help.

Modifications made to the product, unless expressly approved by the party responsible, could void the user's right to operate the equipment.

RF Exposure

This device has been tested and complies with FCC RF Exposure (SAR) limits in typical laptop computer configurations and this device can be used in desktop or laptop computers with side mounted PCMCIA slots, which can provide 1 cm separation distance from the antenna to the body of the user or a nearby person. Thin laptop computers may need special attention to maintain antenna spacing while operating. This device cannot be used with handheld PDAs (personal digital

assistants). Use in other configurations may not ensure compliance with FCC RF exposure guidelines. This device and its antenna must not be co-located or operate in conjunction with another antenna or transmitter.

Safety Summary Messages

WARNING HIGH VOLTAGE



**If used in the equipment.
Make sure equipment is properly grounded BEFORE
opening. Failure to observe safety precautions may
result in Electrick Shock to user.**



CAUTION

**Check voltages before connecting equipment to power
supplies. Wrong voltages applied may result in damage
to equipment.**

Chapter 2 About this Manual

2.1 Introduction

This manual provides a general product overview and description of the subsystems, components, basic operation and preventive maintenance instructions of the Lynx L-510.

2.2 Scope and Purpose

This manual provides the following:

- An overview of the Lynx L-510 system configuration and connectivity;
- General description and specifications of the Lynx L-510 system components;
- Operating instructions of the system and equipment;

2.3 Targeted Audience

This manual is designed and developed for the operators and users who are required to operate and perform first-level maintenance of the Lynx L-510. It assumes the user of this manual has basic knowledge and experience in operating similar modem configuration and computer systems equipment.

2.4 Manual Organization

The manual is divided into the following chapters:

1. *Chapter 1 – About this Manual*; this chapter provides an introduction to the manual's scope and purpose, targeted audience and contents organization.
2. *Chapter 2 – ADSL Ethernet Router Description*; this chapter provides the system configuration diagram description on the system support features.
3. *Chapter 3 – Your Gateway At A Glance*; this chapter provides an overview of the system configuration, composition, connectivity, introduction and general description of the Lynx L-510.
4. *Chapter 4 – Installing the Lynx L-510*; this chapter provides description of the Lynx L-510 installation *process*.
5. *Chapter 5 – Setting Up the Lynx L-510*; this chapter provides description of all function within the Web User Interface.

Chapter 3 ADSL Ethernet Router Description

The Lynx L-510 ADSL2/2+ LAN 802.11g 4 Port Ethernet & USB Combo Router is a high-speed WAN bridge/router.

This full-featured product is specifically designed to allow maximum of 4 Ethernet-workstations to be connected to the Internet and directly connect to your local area network via high speed 10/100 Mbps Ethernet. Users using wireless workstations will be able to connect to the Internet using 802.11g wireless technology. The Lynx L-510 has also full NAT firewall and DMZ services to block unwanted users from accessing your network.

For game users, the Lynx L-510 had already pre configured for several low latency game ports. Just click on the game you are playing on line and the rest is done for you.

The Lynx L-510 is fully compatible with all PCs; as long as the PC supports an Ethernet interface and is running a TCP/IP protocol stack, your PC can have high-speed WAN access. So, plug in the Lynx L-510, configure it and enjoy the fast Internet access like never before.

3.1 Features

ADSL/ATM Support

- ANSI T1.413 issue 2, ITU-T G.992.1 (G.dmt) and G.992.2 (G.lite) compliant
- ADSL2, ADSL2+, RE-ADSL compliant
- Rate Adaptive modem at 32 Kbps steps
- Dynamic Adaptive Equalization to improve Carrier's service area
- Bridge Tap Mitigation support
- ATM Layer with Traffic shaping QoS Support (UBR, CBR, VBR-rt, VBR-nrt)
- AAL ATM Attributes - AAL5
- Multiple PVC up to 8 support (Bridge Support)
- Spectral compatibility with POTS
- F5 OAM Loopback/Send and Receive

Encapsulation Support

- RFC2684 Bridge and Routed LLC and VC Mux support
- RFC2364 PPPoA Client support
- RFC2516 PPPoE Client support
- RFC2225/RFC1577 Classical IP Support
- Transparent Bridge Support
- PAP/CHAP/MS-CHAP for Password Authentication support

Network Support

- Static IP, Dynamic RIP routing support
- IP/TCP/UDP/ICMP/ARP/RARP Application Support
- Network Address Translation (NAT)
- Port Mapping/Forwarding
- Easy setup of Port Forwarding rules for popular Games/Application
- NAT Application Level Gateway for popular applications
- DHCP Server/Relay/client
- DMZ support
- Single Session IP Sec and PPTP/L2TP VPN pass through support
- PPP Always on with configurable timeout
- PPP Dial on Demand

Management Support

- Web Based HTTP management GUI
- TFTP/FTP Support for Firmware Upgrade
- Web Based Firmware Upgrade (Local)
- Soft Factory Reset Button via Web GUI
- Diagnostic Test (DSL, OAM, Network, Ping Test)
- Telnet/CLI (Read Only)
- Syslog Support

Security Support

- NAT for basic Firewall support
- Packet Filtering Firewall Support
- Stateful Packet Inspection Support
- Protection against Denial of Service attacks
- Password Authentication to Modem

WLAN Support

- 802.11, 802.11b and 802.11g compliant
- Support seamless WLAN roaming
- Frequency Band : 2412 MHz - 2462 MHz (North America/FCC)
- 2412 MHz - 2472 MHz (ETSI/Europe)
- 2412 MHz - 2484 MHz (Japan) 2457 MHz - 2472 MHz (France)
- 2457 MHz – 2462 MHz (Spain)

-
- Supports Direct Sequence Spread Spectrum (DSSS) technology
 - Modulation: OFDM with BPSK,QPSK, 16QAM, 64QAM, DBPSK, DQPSK, CCK
 - Wireless Media Access Protocol- CSMA/CA with ACK
 - Dynamic Rate Scaling from 54, 48, 36, 24, 12, 11, 9, 6, 5.5, 2, 1 Mb/s
 - Operating Range of >300 Meters (Open Air)

External Connectors

- 1 x RJ-11 Telephone socket for ADSL line
- 4 x RJ45 for 10/100Base-T Ethernet (MDI-X)
- 1 x USB 1.1 Type B
- 1 x DC Jack for Power Input
- 1 x Factory Default Reset Button
- 1 On/Off Power Switch (Population Option)

3.2 Lynx L-510 Overview

Fig 1-1 shows the system configuration diagram of a typical Lynx L-510 connection.

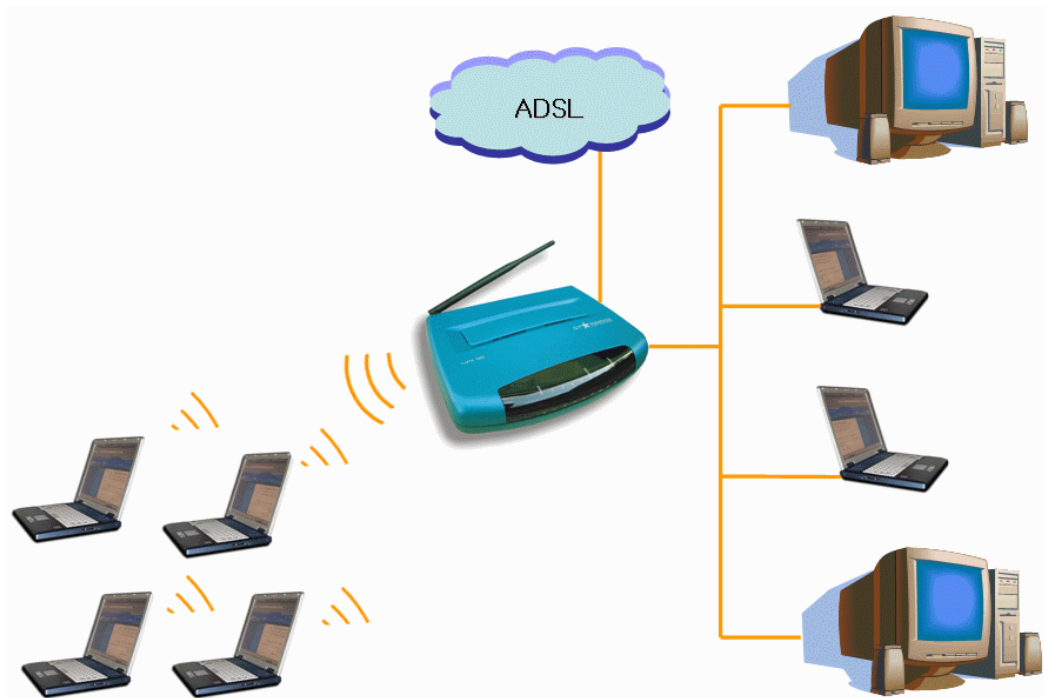


Figure 1-1: Lynx L-510 Configuration Diagram

Chapter 4 Your Gateway At A Glance

The Lynx L-510 has different ports and LEDs. Let's take a look at the different options.

4.1 Ports and Buttons

Reset and Restore to Factory Defaults: The restore to factory defaults feature will set the Lynx L-510 to its factory default configuration by resetting the Lynx L-510. You may need to place the Lynx L-510 into its factory defaults if the configuration is changed; you lose the ability to interface to the Lynx L-510 via the web interface, or following a software upgrade. To reset the Lynx L-510, simply press the reset button for about ~ 10 seconds. The Lynx L-510 will be reset to its factory defaults and after about 30 ~ 40 seconds the Lynx L-510 will become operational again.

LAN (local area network) ETHERNET port (E1-E4): connects to Ethernet network devices, such as a PC, hub, switch, or routers. The ports are 10/100 Base-T Auto-MDI/MDIX (allows either cross or straight cable).

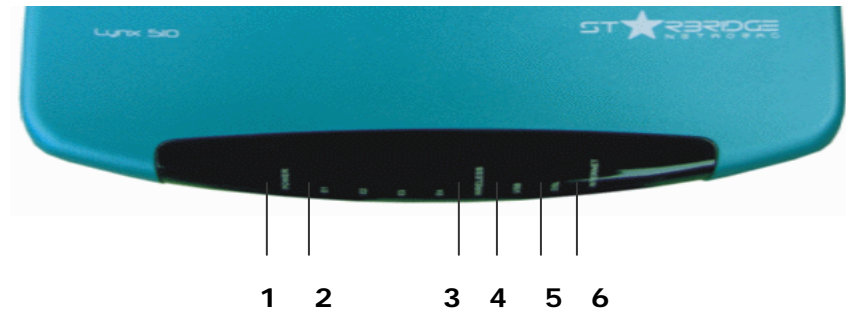
Power is where you connect the power. Make sure to observe the proper power requirements. The required power is 9 volts.

USB (universal serial port): connects to a PC's USB port.

DSL port: This is the WAN interface that connects directly to your phone line.

4.2 Lynx L-510 Overview

Front Indicators



1 POWER

Lights up when power is supplied to the ADSL Router.

2 ETHERNET (E1 ~ E4)

Lights up when the Ethernet cable is properly connected from your ADSL Router to the Ethernet Card. It flickers when the ADSL is transmitting/receiving data.

3 WIRELESS

Flickers when the Wireless LAN is operational.

4 USB

Lights up when the USB cable is properly connected from your ADSL Router to the USB slot. Lights Off when the USB cable is not connected or it is properly disconnected.

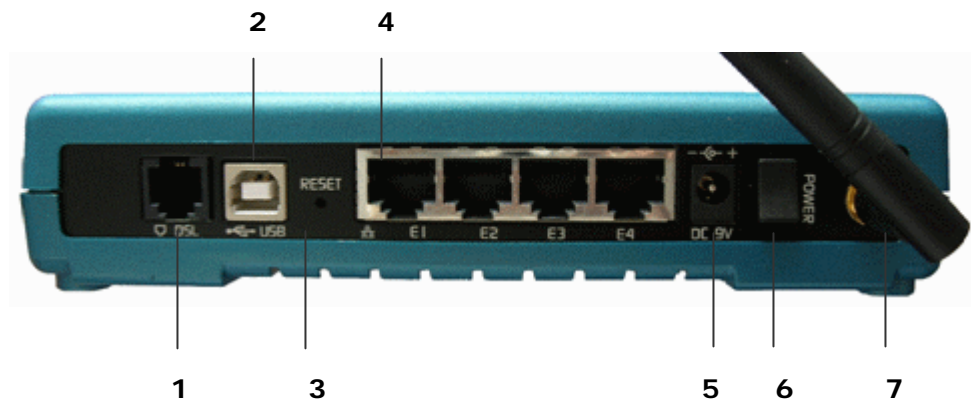
5 DSL

LED lights off when no Telephone jack (RJ-11) is connected. Flickers when the ADSL Router is trying to establish a connection with the ADSL Service Provider (Training). **Steady Green LED lights up** when the ADSL connection is established.

6 Internet

Green LED lights up when the PPP connection is established. Lights off when no PPP connection.

Back Panel



1 DSL

Connect the telephone jack (RJ-11) to your Telephone Wall Socket (DSL line).

2 USB

Connect the USB jack to your PC's USB slot.

3 RESET

To reset your ADSL Router to factory default settings (all customized settings that you have saved will be lost!). To reset the ADSL Router, simply press the reset button for about 10 seconds.

4 ETHERNET (E1-E4)

10/100 Base-T Auto-MDI/MDIX Ethernet jack (RJ-45) to connect to your PC's Ethernet Network card or Ethernet Hub / Switch.

5 DC 9V

To connect to the Power Adapter that comes with your package.

6 POWER SWITCH

To power on or off the modem. Push downwards to switch ON and lift upwards to OFF.

7 RF Antenna

180° 2.4Ghz Wireless Antenna.

Chapter 5 Installing The Lynx L- 510

1. Locate a suitable location for the Lynx L-510. For connections to the USB, Ethernet and DSL interfaces, please refer to the **Quick Guide**.
2. Connect the AC Power Adapter. Depending upon the type of network, you may want to put the power supply on an uninterruptible supply (UPS).



Note: Please use the power adapter supplied with the Lynx L-510. A different adapter may damage the product.

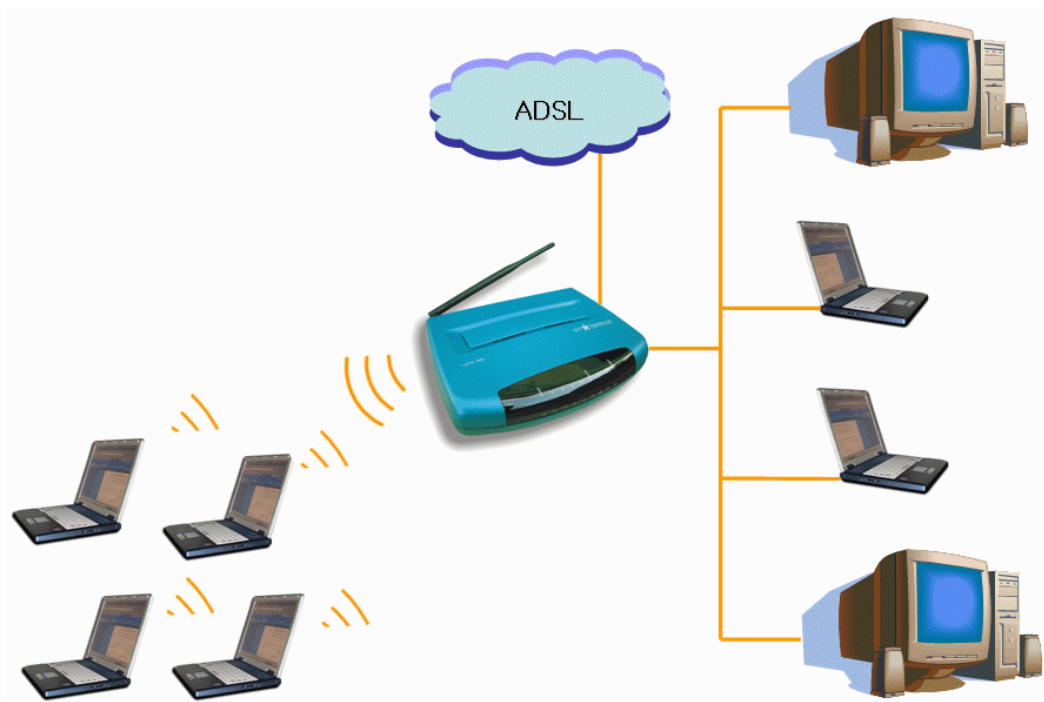


Figure 1-2: Lynx L-510 Connection Diagram

Chapter 6 Setting Up the Lynx L-510

The basic tabs consist of features which are catered for basic users.

This section will guide you through your Lynx L-510's configuration. The Lynx L-510 is shipped with a standard PPP configuration.

6.1 Logging into your Lynx L-510

To configure your Lynx L-510, open your web browser. You may get an error message at this point; this is normal.

1. Type the default IP address (**192.168.1.1**) or **login.router on** on the web address bar.
2. Press the **Enter** key and the following screen will appear.



Note: Before sitting up your Lynx L-510, make sure you have followed the steps detailed in your easy start guide. You should have your computer configured for DHCP mode and have proxies disabled on your browser. Upon accessing the Lynx L-510, if the browser still displays a login redirection screen, you should check your browser's settings and ensure that the JavaScript support is enabled. If the screen shown in Figure 1-5 is not attainable, you must delete your temporary Internet files to clear the web cache.

Figure 1-3: Setup Page

Upon entering the default IP address or the short-cut name (login.router), if the user is first time login, the user will be brought to the “Quick Start” page. See **Fig 1.5**. The Quick Start page is meant for basic users whom only require easy connectivity to the Internet without worrying about any other advance configuration setting. If you are in doubt for what content to enter for the Protocol, VPI and VCI, please contact your Service Provider for assistance.

For those who have their routers configured, you will be directed to the “Basic Home” page. See **Fig 1-6**.

The screenshot shows the 'Basic Home' page of a Starbridge router. The top navigation bar includes links for 'Save Settings', 'Restart Access Point', 'Restart Router', 'Basic' (highlighted with a red circle), 'Advanced', 'Wireless', 'Security', 'Status', and 'Help'. The left sidebar contains a menu with 'Basic', 'Home', 'Setup', 'LAN Configuration', and 'Diagnostics'. The main content area is titled 'Basic Home' and contains four tables of configuration data.

Connection Information		Router Information	
DSL	UP	System Uptime	0 hours 5 minutes
Downstream / Upstream (Kbps)	3488/576	Model	Lynx510
Internet	Connected	Serial Number	none
Connected Time	0hr 0min 9sec	Firmware Version	73.48.2
Connection Type	PPPoA	Ethernet MAC address	00:e0:a0:a6:66:70
Username	username@isp	DSL MAC address	N/A
IP Address	220.255.91.204	USB MAC address	00:E0:A6:66:41:EB
Default Gateway	220.255.161.1	AP MAC	00:50:f1:12:12:10
Primary DNS	165.21.83.88	NAT	Enabled
Secondary DNS	165.21.100.88	Firewall	Enabled
Disconnect			

Local Network		Wireless Network	
LAN IP Address	192.168.1.1	Network Name / SSID	Starbridge
DHCP	Enabled	Security Type	None
DHCP Range	192.168.1.10 - 192.168.1.40	WEP Encryption Key	Disabled
Ethernet	Connected		
USB	Disconnected		

Figure 1-4: Basic Home Screen

6.2 Basic

If you have already configured your router and wish to change your current configuration, click on the ‘Setup’ link. **Fig 1-7** will appear.

Save Settings
Restart Access Point
Restart Router
Basic
Advanced
Wireless
Security
Status
Help

Basic
Home
Setup
LAN Configuration
Diagnostics

Connection Information
Router Information

DSL
UP

Downstream / Upstream (Kbps)
3488/576

Internet
Connected

Connected Time
0hr 0min 9sec

Connection Type
PPPoA

Username
username@isp

IP Address
220.255.91.204

Default Gateway
220.255.161.1

Primary DNS
165.21.83.88

Secondary DNS
165.21.100.88

Disconnect

System Uptime
0 hours 5 minutes

Model
Lynx510

Serial Number
none

Firmware Version
73.48.2

Ethernet MAC address
00:e0:a0:a6:66:70

DSL MAC address
N/A

USB MAC address
00:E0:A6:66:41:EB

AP MAC
00:50:f1:12:12:10

NAT
Enabled

Firewall
Enabled

Local Network
Wireless Network

LAN IP Address
192.168.1.1

DHCP
Enabled

DHCP Range
192.168.1.10 - 192.168.1.40

Ethernet
Connected

USB
Disconnected

Network Name / SSID
Starbridge

Security Type
None

WEP Encryption Key
Disabled

Figure 1-5: Basic Home Page

Click on Apply after entering your settings and then click on Save.

Note: after clicking on Apply, please be sure to click on “Save” to register the username/password or any other changes.

6.2.1 LAN / DHCP Configuration

On one side of your Lynx L-510, you have your own Local Area network (LAN) connections. This is where you plug in your local computers to the Lynx L-510. The Lynx L-510 is normally configured to automatically provide all the PC's on your network with Internet addresses.

To enable or disable DHCP, Click setup. Under LAN Setup, select DHCP Configuration. This will bring up the screen shown in **Fig 1-8**. The Start IP Address is where the DHCP server starts issuing IP addresses. This value must be greater than the Lynx L-510 IP address value. For example if the Lynx L-510 IP address is 192.168.1.1 (default) than the starting IP address must be 192.168.1.2 (or higher). The End IP Address is where the DHCP server stops issuing IP addresses. The ending address cannot exceed a subnet limit of 254. Hence the max value for our default gateway is

17

192.168.1.254. If the DHCP server runs out of DHCP addresses, users will not get access to network resources. If this happens you can increase the Ending IP address (to the limit of 255) or reduce the lease time. The Lease Time is the amount of time a network user will be allowed connection to the Lynx L-510 with their current dynamic IP address. The amount of time is in units of minutes; the default value is 3600 minutes (60 hours). Note: If you change the start or end values, make sure the values are still within the same subnet as the gateways IP address. In other words, if the gateways IP address is 192.168.1.1 (default) and you change the DHCP start/end IP addresses to be 192.128.1.2/192.128.1.100, you will not be able to communicate to the Lynx L-510 if your PC has DHCP enabled. In addition to the DHCP server feature, the Lynx L-510 supports the DHCP relay function. When the Lynx L-510 is configured as DHCP server, it assigns the IP addresses to the LAN clients. When the Lynx L-510 is configured as DHCP relay, it is responsible for forwarding the requests and responses negotiating between the DHCP clients and the server.

By turning off the DHCP server and relay the network administrator must carefully configure the IP address, Subnet Mask and DNS settings of every computer on your network. Do not assign the same IP address to more than one computer and your Lynx L-510 must be on the same subnet as all the other computers.

The screenshot displays the Starbridge Network configuration web interface. The top navigation bar includes links for 'Save Settings', 'Restart Access Point', 'Restart Router', and tabs for 'Basic', 'Advanced', 'Wireless', 'Security', 'Status', and 'Help'. The left sidebar shows a menu with 'Basic' selected, and 'LAN Configuration' highlighted with a red circle. The main content area is titled 'LAN Group 1 Configuration' and contains the following fields and options:

- IP Address: 192.168.1.1
- Netmask: 255.255.255.0
- Default Gateway: (empty field)
- Host Name: login
- Domain: Starbridge
- ☒ Enable DHCP Server
 - Start IP: 192.168.1.10
 - End IP: 192.168.1.40
 - Lease Time: 3600 Seconds
- ☐ Enable DHCP Relay
 - Relay IP: 20.0.0.3
- ☐ Server and Relay Off

At the bottom right of the configuration area are 'Apply' and 'Cancel' buttons.

Figure 1-6: LAN / DHCP Configuration

6.2.2 Diagnostic Test

Diagnostic Test is used for investigating whether the Lynx L-510 is properly connected to the WAN Network. See **Fig 1-9**. This test may take a few seconds to complete. To perform the test, select your connection from the list and press the Test button. Before running this test, make sure you have a valid DSL link.

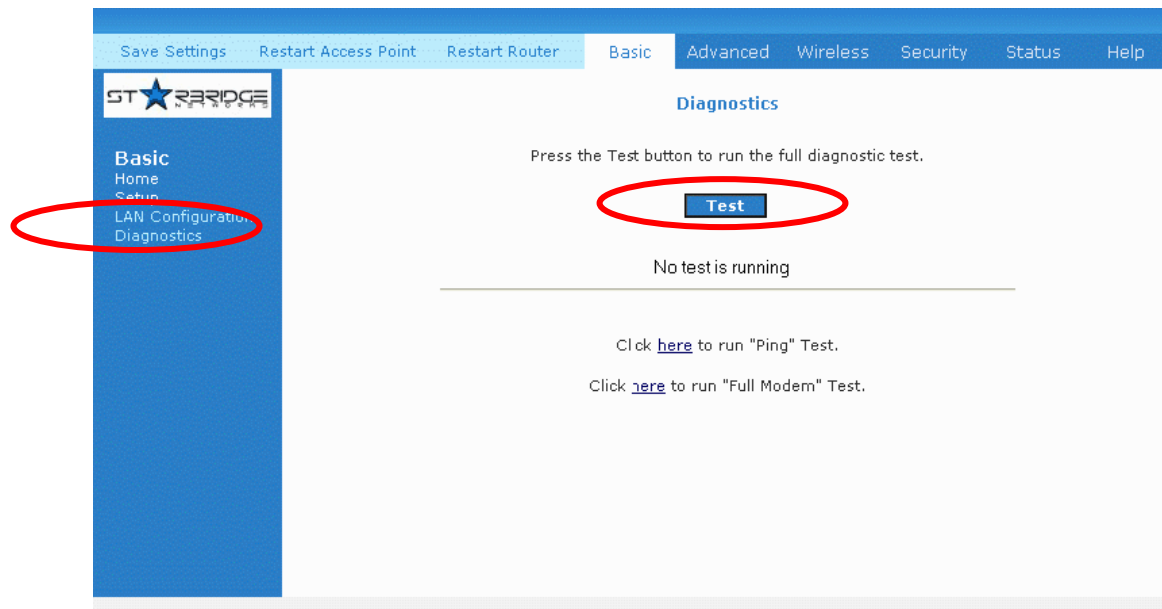


Figure 1-7: Diagnostics Test Screen

After running the Diagnostic Test, the screen will indicate that the portion which pass or fail the test. Please click on the **Help** links, which will provide remedy to the problem as shown in **Fig 1-10**. The purpose of the “Fix It” button is to restore the router’s VPI and VCI to its originated setting.

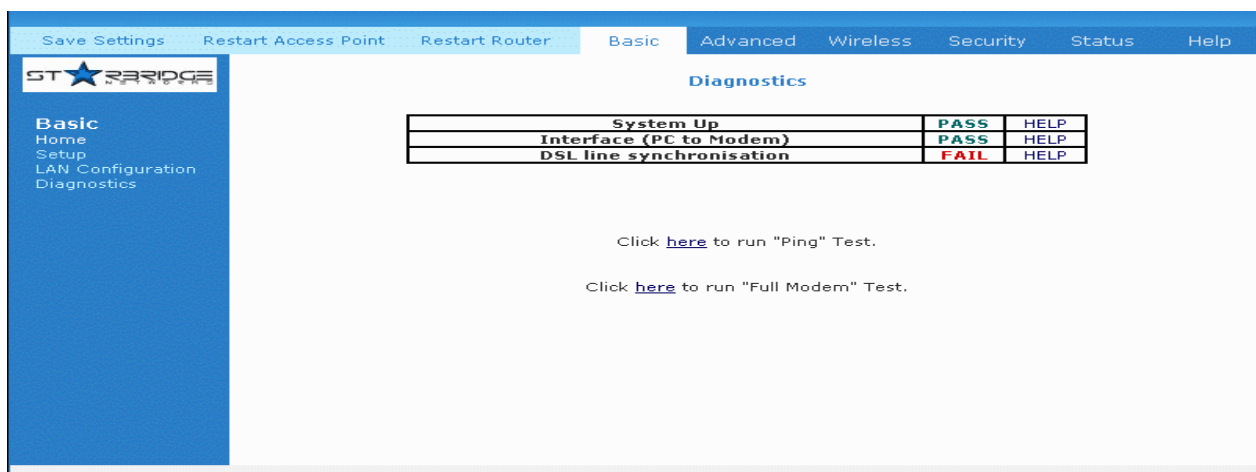


Figure 1-8: Diagnostic Test Result screen

6.2.3 Ping Test

Once you have your Lynx L-510 configured, ensure you can ping the network. You can access the Ping Test page by clicking on the “**here**” hyperlink in Diagnostic Page. Type the target address that you want to ping. If your PC is connected to the Lynx L-510 via the default DHCP configuration, you should be able to Ping the network address 192.168.1.1. See **Fig 1-11**. If your ISP has provided their server address, try to ping the address. If the pings for both the WAN and the LAN sides are complete and you have the proper protocols configured, you should be able to surf the Internet. By default when you select ping test, the Lynx L-510 will ping itself 3 times. The Lynx L-510 passed the Ping test; this basically means that the TCP/IP protocol is up and running. If this first Ping test does not pass, the TCP/IP protocol is not loaded for some reason; you should restart the Lynx L-510.

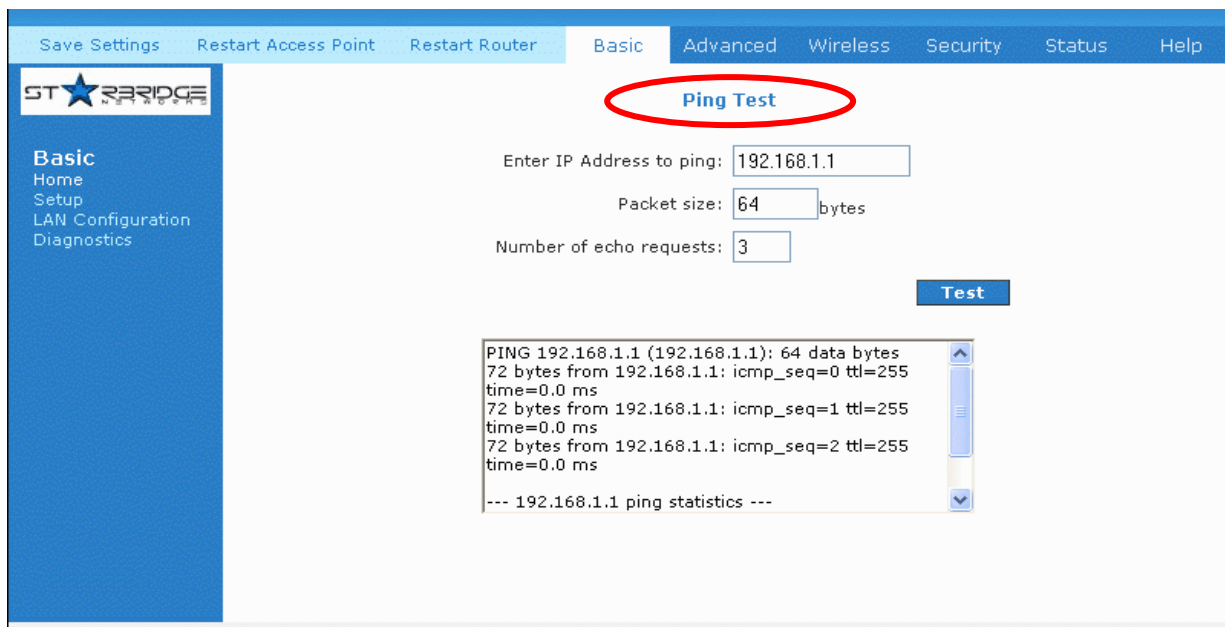


Figure 1-9: Ping Test Screen 2010664daniela quvedo

6.2.4 Modem Test

This test can be used to check whether your Modem is properly connected to the Network. Select your connection from the list and press the ‘**Test**’ button. See **Fig 1-12**.

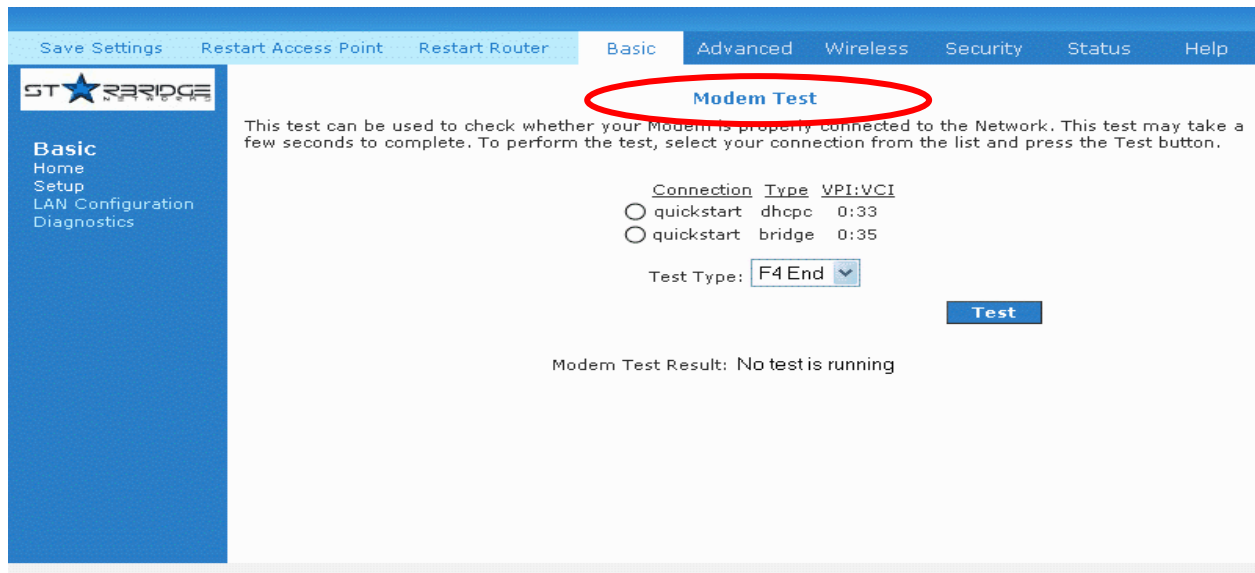


Figure 1-10: Modem Test

6.3 Advanced

This mode is catered for advance users, a brief explanation of the links are listed as shown below.

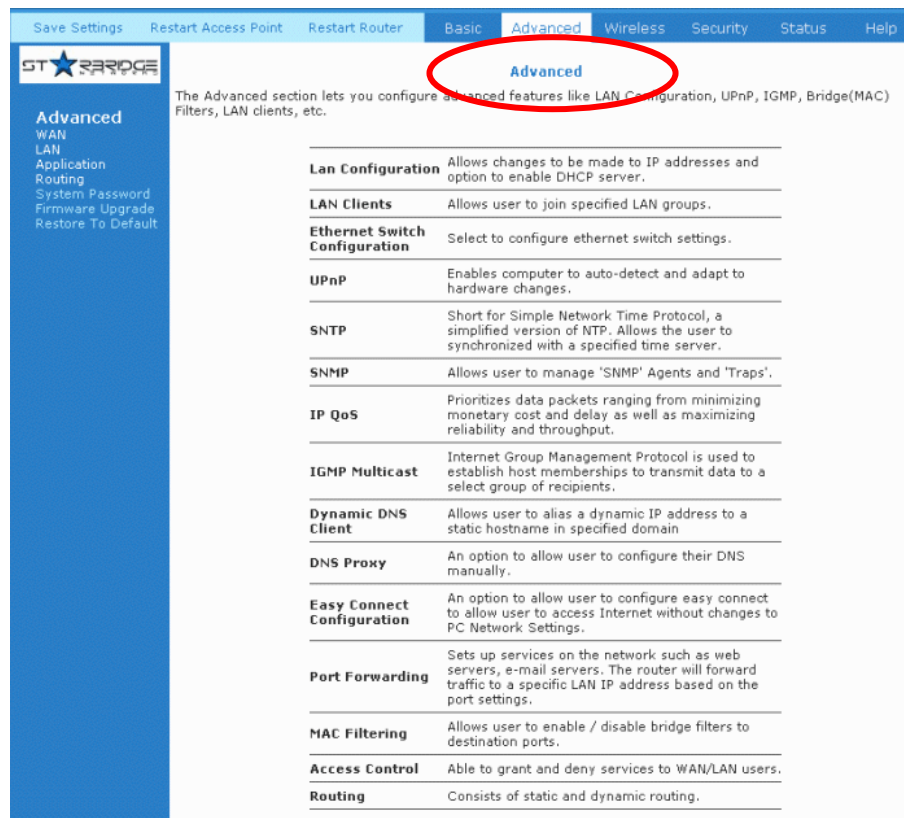


Figure 1-11: Advanced Screen

6.3.1 WAN Connection

On the other side of the Lynx L-510 is where your Wide Area Network (WAN) connection; also referred to as a broadband connection. This WAN connection is different for every WAN supplier. Most of the configuration you will perform will be in this area. Local Area Network Connection(s).

6.3.2 New Connection

A new connection is basically a virtual connection. Your Lynx L-510 can support up to 8 different (unique) virtual connections. If you have multiple different virtual connections, you may need to utilize the static and dynamic routing capabilities of the modem to pass data correctly.

The screenshot displays the 'PPPoE Connection Setup' page. At the top, there are tabs: 'Save Settings', 'Restart Access Point', 'Restart Router', 'Basic', 'Advanced' (selected), 'Wireless', 'Security', 'Status', and 'Help'. On the left, a sidebar shows 'Advanced' settings: WAN, LAN, Application, Routing, System Password, Firmware Upgrade, and Restore To Default. The main content area is titled 'PPPoE Connection Setup'. It includes a 'Name' field (circled in red), a 'Type' dropdown set to 'PPPoE' (circled in red), and a 'Sharing' dropdown set to 'Disable'. Below these are 'Options' (checked for NAT and Firewall), 'VLAN ID' (0), and 'Priority Bits' (0). The 'PPP Settings' section contains fields for 'Username' (username), 'Password' (masked with dots), 'Idle Timeout' (60 secs), 'Keep Alive' (10 min), 'Authentication' (radio buttons for Auto, CHAP, PAP), 'MTU' (1492 bytes), 'On Demand' (checkbox), 'Default Gateway' (checked), 'Enforce MTU' (checked), 'Debug' (checkbox), 'PPP Unnumbered' (checkbox), and 'LAN' (dropdown set to 'LAN group'). The 'PVC Settings' section includes 'PVC' (dropdown set to 'New', circled in red), 'VPI' (0), 'VCI' (0), 'QoS' (dropdown set to 'UBR'), 'PCR' (0 cps), 'SCR' (0 cps), 'MBS' (0 cells), 'CDVT' (0 usecs), and 'Auto PVC' (checkbox). At the bottom, there are 'Connect' and 'Disconnect' buttons, and a row of 'Apply', 'Delete', and 'Cancel' buttons.

Figure 1-12: New Connection (PPPOE Connection Setup)

6.3.3 ADSL Modulation

To configure the DSL modulation type, Click setup. Under WAN Setup, select Modem Setup. This will bring up the modem setup screen. Leave the default value if you are unsure or the DSL/ISP did not provide this information. For most all cases, this screen should not be modified.

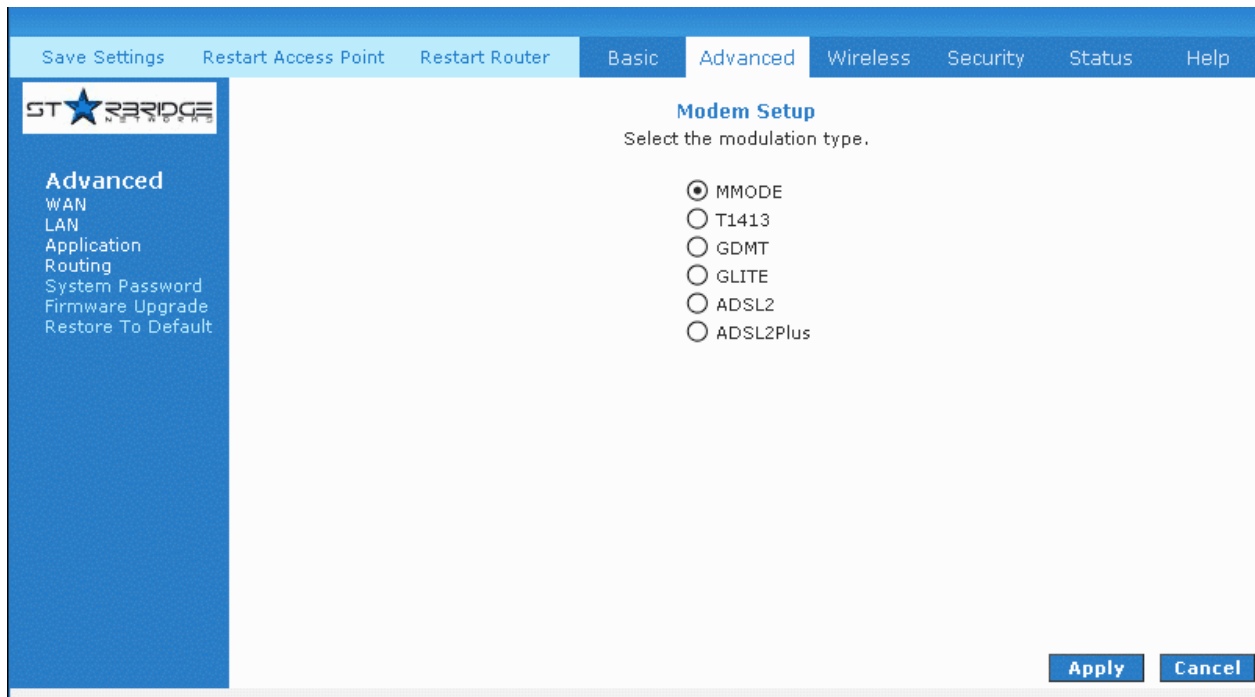


Figure 1-13: ADSL Modulation (Modem Setup)

6.3.4 Quickstart

PPPoE is also known as RFC 2516. It is a method of encapsulating PPP packets over Ethernet. PPP or Point-to-Point protocol is a method of establishing a network connection/session between network hosts. It usually provides a mechanism of authenticating users.

To configure the gateway for PPPoE, click on Setup and then click on New Connection. The default PPPoE connection setup is displayed. At the Type field select PPPoE and the PPPoE connection setup page is displayed. Give your PPPoE connection a unique name; the name must not have spaces and cannot begin with numbers. In this case the unique name is called PPPoE1. Select the encapsulation type (LLC or VC); if you are not sure just use the default mode. Select the VPI and VCI settings; your DSL service provider or your ISP will supply these; in this case the DSL service provider is using 0,100. Also select the quality of service (QOS); leave the default value if you are unsure or the ISP did not provide this information.

Following is a description of the different options:

1. Username: The username for the PPPoE access; this is provided by your DSL service provider or your ISP.

2. Password: The password for the PPPoE access; this is provided by your DSL service provider or your ISP.
3. On-Demand: Enables on-demand mode. The connection will disconnect if no activity is detected after the specified idle timeout value.
4. Idle Timeout: Specifies that PPPoE connection should disconnect if the link has no activity detected for n seconds. This field is used in conjunction with the On-Demand feature. To ensure that the link is always active, enter a 0 in this field.
5. Keep Alive: When on-demand option is not enable, this value specifies the time to wait without being connected to your provider before terminating the connection. To ensure that the link is always active, enter a 0 in this field.
6. Set Route: Specify this connection as the default-route.
7. Enforce MTU: Check this box if you experience problems accessing the Internet over a PPPoE connection. This feature will force all TCP traffic to conform with PPP MTU by changing TCP Maximum Segment Size to PPP MTU.

The screenshot displays the 'PPPoE Connection Setup' page in the STERIDGE Networks web interface. The top navigation bar includes 'Save Settings', 'Restart Access Point', 'Restart Router', and tabs for 'Basic', 'Advanced' (selected), 'Wireless', 'Security', 'Status', and 'Help'. A left sidebar lists 'Advanced' settings: WAN, LAN, Application, Routing, System Password, Firmware Upgrade, and Restore To Default. The main configuration area is divided into several sections:

- General Settings:** Name: quickstart, Type: PPPoE, Sharing: Disable. Options: ☒ NAT, ☒ Firewall. VLAN ID: 0, Priority Bits: 0.
- PPP Settings:** Username: username, Password: masked with dots. Idle Timeout: 60 secs, Keep Alive: 10 min. Authentication: Auto (selected), CHAP, PAP. MTU: 1492 bytes. On Demand: ☐, Default Gateway: ☒. Enforce MTU: ☒, Debug: ☐. PPP Unnumbered: ☐, LAN: LAN group.
- PVC Settings:** PVC: New, VPI: 0, VCI: 35, QoS: UBR. PCR: 0 cps, SCR: 0 cps, MBS: 0 cells, CDVT: 0 usecs, Auto PVC: ☐.

At the bottom, there are buttons for 'Connect', 'Disconnect', 'Apply', 'Delete', and 'Cancel'.

Figure 1-14: Quickstart (PPPOE Connection Setup)

6.3.5 LAN Configuration (VLAN)

The Virtual LANs (VLANs) is a group of devices on different physical LAN segments, which can communicate with each other as if there are all in the same physical LAN segment. VLANs provide a number of benefits over the network. Refer to Figure 1-17.

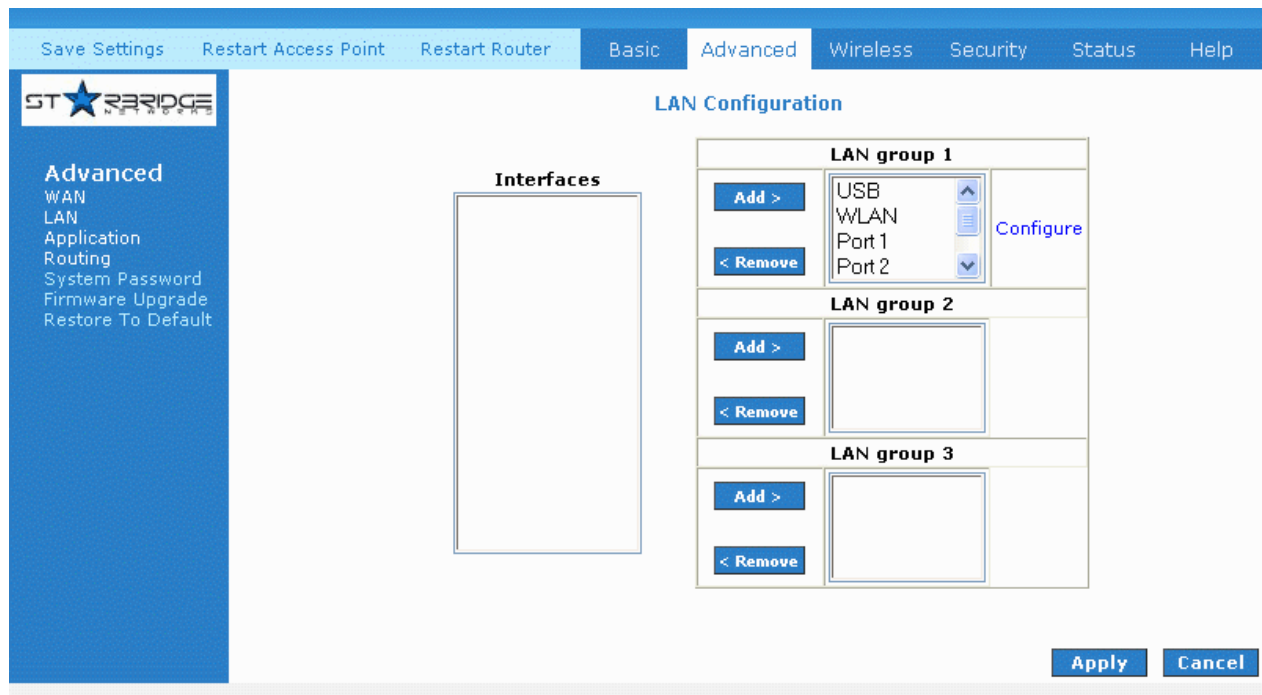


Figure 1-16: LAN Configuration (VLAN)

For example, the modem has 3 bridge PVCs configured.

Refer to **Figure 1-17** and **1-18**.

- Data – 0/35
- VoIP – 0/36
- Manage – 0/88

Figure 1-17 : Create New bridge PVC

Figure 1-18 : Three bridge PVCs are created

Upon creation, the bridge PVCs are attached to LAN Group 1. They can be moved to other LAN Groups by selecting the name, clicking Remove beside the LAN Group, select again from the Interfaces box and clicking Add beside the new LAN Group.

Ports 1 and 3 (denoted by VLAN1 and VLAN3) are bridged to the Data PVC in LAN Group 1.

Ports 2 and 4 (denoted by VLAN2 and VLAN4) are bridged to the VoIP PVC in LAN Group 2.

The Manage PVC is alone in LAN Group 3.

Ports 1 and 3 will get traffic from Data and vice-versa. Ports 2 and 4 will not see traffic from Ports 1, 3 and Data nor the other way round.

You can change the ADSL Router's IP address by clicking on the Configure.

Your ADSL Router's default IP address and subnet mask are 192.168.1.1/255.255.255.0; this subnet mask will allow the ADSL Router to support 254 users. If you want to support a larger number of users you can change the subnet mask; but remember. The DHCP server is defaulted to only give out 255 IP addresses. Further remember that if you change your gateways' IP address and you have DHCP enabled, the DHCP configuration must reside within the same subnet The default gateway is the routing device used to forward all traffic that is not addressed to a station within the local subnet. Your ISP will provide you with the default gateway Address.

The hostname can be any alphanumeric word that does not contain spaces. The domain name is used to in conjunction with the host name to uniquely identify the gateway. To access the ADSL Router's web pages the user can type 192.168.1.1 (the default IP address) or type mygateway.ar7. The apply button will temporarily save this connection. To make the change permanent you need to click on Save Settings. Refer to **Figure 1-19**.

The screenshot displays the StarBridge ADSL Router's web interface. The top navigation bar includes links for 'Save Settings', 'Restart Access Point', 'Restart Router', and tabs for 'Basic', 'Advanced' (selected), 'Wireless', 'Security', 'Status', and 'Help'. The left sidebar shows a menu with 'Advanced' selected, along with options like 'WAN', 'LAN', 'Application', 'Routing', 'System Password', 'Firmware Upgrade', and 'Restore To Default'. The main content area is titled 'LAN Group 1 Configuration' and contains the following sections:

- IP Settings:** Includes radio buttons for 'Unmanaged', 'Obtain an IP address automatically', and 'PPP IP Address'. It also features input fields for 'IP Address' and 'Netmask' with 'Release' and 'Renew' buttons.
- Static IP Configuration:** A section for 'Use the following Static IP address' with input fields for 'IP Address' (192.168.1.1), 'Netmask' (255.255.255.0), 'Default Gateway', 'Host Name' (login), and 'Domain' (router).
- DHCP Server:** Includes a radio button to 'Enable DHCP Server' with associated input fields for 'Start IP' (192.168.1.10), 'End IP' (192.168.1.40), and 'Lease Time' (3600 Seconds).
- DHCP Relay:** Includes a radio button to 'Enable DHCP Relay' with a 'Relay IP' input field (20.0.0.3).
- Services and Status:** A table on the right showing the status of various services: IP Filters (green), Bridge Filters (red), UPnP (red), LAN Clients (green), IP QoS (green), and Static Routing (red).

At the bottom right, there are 'Apply' and 'Cancel' buttons.

Figure 1-19 : Configure

6.3.6 LAN Clients

To add a LAN client select LAN clients, under LAN. If DHCP is used, all DHCP clients are automatically assigned. If a fixed IP address server is on the LAN and you want this server to be visible via the WAN, you must add its IP address. Once the IP address has been added to you can apply Port Forwarding and Access Control rules to this IP address.

The screenshot shows the STARRIDGE router configuration interface. The top navigation bar includes links for Save Settings, Restart Access Point, Restart Router, Basic, Advanced (selected), Wireless, Security, Status, and Help. The left sidebar lists various configuration options under the Advanced tab: WAN, LAN, Application, Routing, System Password, Firmware Upgrade, and Restore To Default. The main content area is titled 'LAN Clients' and includes the instruction: 'To add a LAN Client, Enter IP Address and Hostname, then click Apply.' Below this, there are input fields for 'Select LAN Connection' (set to 'LAN group 1'), 'Enter IP Address', 'Hostname', and 'MAC Address'. A section titled 'Dynamic Addresses' contains a table with columns for Reserve, IP Address, Hostname, MAC, and Type. The table lists one entry: 192.168.1.10, computer, 00:a0:d2:1c:4b:52, Dynamic. At the bottom right, there are 'Apply' and 'Cancel' buttons.

Reserve	IP Address	Hostname	MAC	Type
<input type="checkbox"/>	192.168.1.10	computer	00:a0:d2:1c:4b:52	Dynamic

Figure 1-20: LAN Clients

6.3.7 Ethernet Switch Configuration

The IGMP Snooping prevents the switch from flooding the LAN ports with multicast frames, and will instead direct them to the CPU port for processing. Users are able to specify connection speed and set their values accordingly from the following available options. See Fig 1-21.

- Auto
- 10/Half Duplex
- 10/Full Duplex
- 100/Half Duplex
- 100/Full Duplex

	Set Value	Fallback Value
Physical Port1:	Auto	100/Full Duplex
Physical Port2:	Auto	Disabled
Physical Port3:	Auto	Disabled
Physical Port4:	Auto	Disabled
IGMP Snooping:	Enable	

Figure 1-21: Ethernet Switch Configuration

6.3.8 Application (UPnP)

UPnP, NAT and Firewall Traversal allow traffic to pass-thru the Lynx L-510 for applications using the UPnP protocol. This feature requires one active DSL connection. In presence of multiple DSL connections, select the one over, which the incoming traffic will be present, for example the default Internet connection.

To enable UPnP, you must first have a WAN connection configured. Once a WAN connection is configured, click Advanced and under Advanced, select UPnP. You must enable UPnP and then select which connection will utilize UPnP. In this case the PPPoA connection is enabled. See **Fig 1-22**.

Figure 1-22: UPnP

6.3.9 SNTP

SNTP (Simple Network Timing Protocol) is a protocol used to synchronize the system time to the public SNTP servers. It uses the UDP protocol on port 123 to communicate between clients and servers. When the SNTP feature is enabled, your DSL600EU will start querying for the time clock information from the primary SNTP server. If it fails to get a valid response within the "timeout" period, it will try for "retry" number of times, before moving to the Secondary SNTP server. If it fails to get a valid response from Secondary SNTP server within valid retry times, it starts querying Tertiary SNTP server. If it fails to get a valid response from all the servers, then the program stops. When a valid response is received from one of the server, the program sleeps for "Polling_interval" amount of minutes, before starting the whole process again.

Use the following procedures to enable SNTP.

1. Check Enable SNTP.
2. Primary SNTP Server - The IP address or the host name of the primary SNTP server.
3. Secondary SNTP Server - The IP address or the host name of the secondary SNTP server.
4. Tertiary SNTP Server - The IP address or the host name of the tertiary SNTP server.
5. Timeout - If the DSL600EU failed to connect to a SNTP server within the 'Timeout' period, it will retry the connection.
6. Polling Interval - Time between a successful connection with a SNTP server and a new attempt to connect to an SNTP server.
7. Retry Count - The number of times the DSL600EU will try to connect to an SNTP server before it try to connect to the next server in line.
8. Time Zone - The time zone of the DSL600EU.
9. Day Light - Check/uncheck this option to enable/disable day light saving. See **Fig 1-23**.

The screenshot shows the ST-RIDGE Networks configuration interface. At the top, there are tabs: Save Settings, Restart Access Point, Restart Router, Basic, **Advanced** (selected), Wireless, Security, Status, and Help. The 'Advanced' tab is further divided into sub-tabs: WAN, LAN, Application, Routing, **SNTP** (circled in red), System Password, Firmware Upgrade, and Restore To Default. The main content area is titled 'To enable SNTP, check the Enable SNTP box and enter a time server.' It includes a checkbox for 'Enable SNTP', three input fields for 'Primary SNTP Server', 'Secondary SNTP Server', and 'Tertiary SNTP Server' (all set to 0.0.0.0), a 'Timeout' field (5 Secs), a 'Polling Interval' field (30 Mins), a 'Retry Count' field (2), a 'Time Zone' dropdown menu (set to (GMT-12:00) International Date Line West), and a 'Day Light' checkbox. At the bottom right, there are 'Apply' and 'Cancel' buttons.

Figure 1-23: SNTP

6.3.10 SNMP

SNMP (Simple Network Management Protocol) is a troubleshooting and management protocol, which uses the UDP protocol on port 161 to communicate between clients and servers. SNMP uses a manager MIB (management information base) agent solution to fulfill the network management needs. The agent is a separate station that can request data from an SNMP agent in each of the different managed system in the network. The agent uses the MIBs as dictionaries of manageable objects. Each SNMP-managed device has at least one agent that can respond to the queries from the NMS. The SNMP agent supports GETS, SETS, and TRAPS for 4 groups with MIB-II: System, Interface, IP, and ICMP. The SNMP agent supports three-community names authentication. See **Fig 24**.

Save Settings

Restart Access Point

Restart Router

Basic


Advanced

Wireless

Security

Status

Help

ST  RIDGE NETWORKS

Advanced

WAN

LAN

Application

Routing

System Password

Firmware Upgrade

Restore To Default

SNMP Management

☒ Enable SNMP Agent

☒ Enable SNMP Traps




Name:

Location:




Contact:

Vendor OID: 1.3.6.1.4.1.294

Community

Name	Access Right
<input type="text" value="public"/>	<input type="text" value="ReadOnly"/> 
<input type="text"/>	<input type="text"/> 
<input type="text"/>	<input type="text"/> 

Traps

Destination IP	Trap Community	Trap Version
<input type="text"/>	<input type="text"/>	<input type="text"/> 
<input type="text"/>	<input type="text"/>	<input type="text"/> 
<input type="text"/>	<input type="text"/>	<input type="text"/> 

Apply

Cancel

Figure 1-24: SNMP Management

6.3.11 IP QoS

When QoS is enabled in the AR7, the designated machine, application or person would have precedence over peers when competing for bandwidth. The IP QoS Setup page allows you to configure QoS for a connection, view previously configured QoS rules, add a new rule, or delete an existing rule. Each output device has three priority queues associated with transmit data. The **high priority** queues have strict priority over the **medium priority** and **low priority** queues, and therefore can exhaust all available bandwidth. The web UI will allow the user to select the weights of the medium and low priority queues in increments of 10 percent so that that the sum of the weights of the 2 queues is equal to 100 percent. These queues will be serviced on a Round Robin priority basis according to the weights assigned, after the high priority queues have been completely serviced. See **Fig 1-25**.

Save Settings

Restart Access Point

Restart Router

Basic

Advanced

Wireless

Security

Status

Help

ST★ARRIDGE

Advanced

WAN

LAN

Application

Routing

System Password

Firmware Upgrade

Restore To Default

IP QoS

Choose a connection: quickstart

Low priority weight: 40%

Medium priority weight: 60%

Enable IPQoS: ☐

Trusted Mode: ☐

	Source	Source	Destination	Destination					
Name	IP	Port Start	IP	Port Start	Protocol	Priority	Phy Port	TOS	Delete
	Mask	Port End	Mask	Port End					

Add

Apply

Cancel

Figure 1-25: IP QoS

6.3.12 IGMP Multicast

If the Lynx L-510 is connected to more than one network, you may need to set up a static route between them. A static route is a pre-defined pathway that network information must travel to reach a specific host or network. You can use static routing to allow different IP domain users to access the Internet through the Lynx L-510.

The New Destination IP is the address of the remote LAN network or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route here. For a standard Class C IP domain, the network address is the first three fields of the New Destination IP, while the last field should be 0. The Subnet Mask identifies which portion of an IP address is the network portion, and which portion is the host portion. For a full Class C Subnet, the Subnet Mask is 255.255.255.0. The Gateway IP address should be the IP address of the gateway device that allows for contact between the Gateway and the remote network or host. The Hop Count determines the maximum number of steps between network nodes that data packets will travel. A node is any device on the network (such as a router or switch). See **Fig 1-26**.

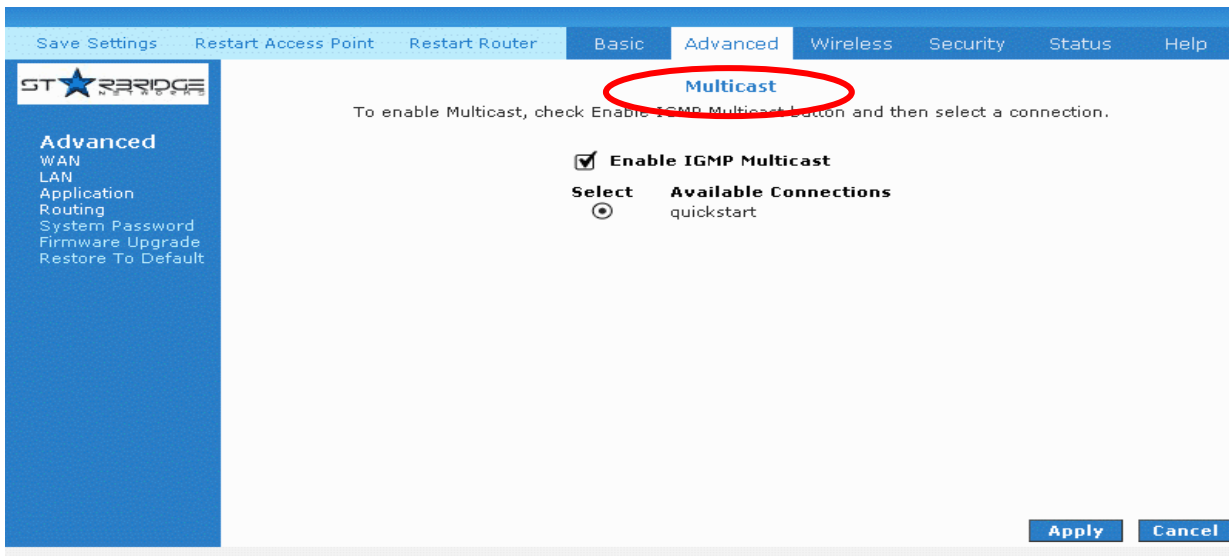


Figure 1-26: IGMP Multicast

6.3.13 Dynamic DNS Client

Dynamic DNS Client allows the user to register with a Dynamic DNS Provider as listed. The dynamic DNS will be linked with the WAN IP of the router even after the ISP update the WAN IP to another IP address. It can be useful in web hosting and FTP services. **See Fig 1-27.**

*Note: The Username/Password entered should be similar to the Username/Password you have specified during the registration of the DNS hostname.

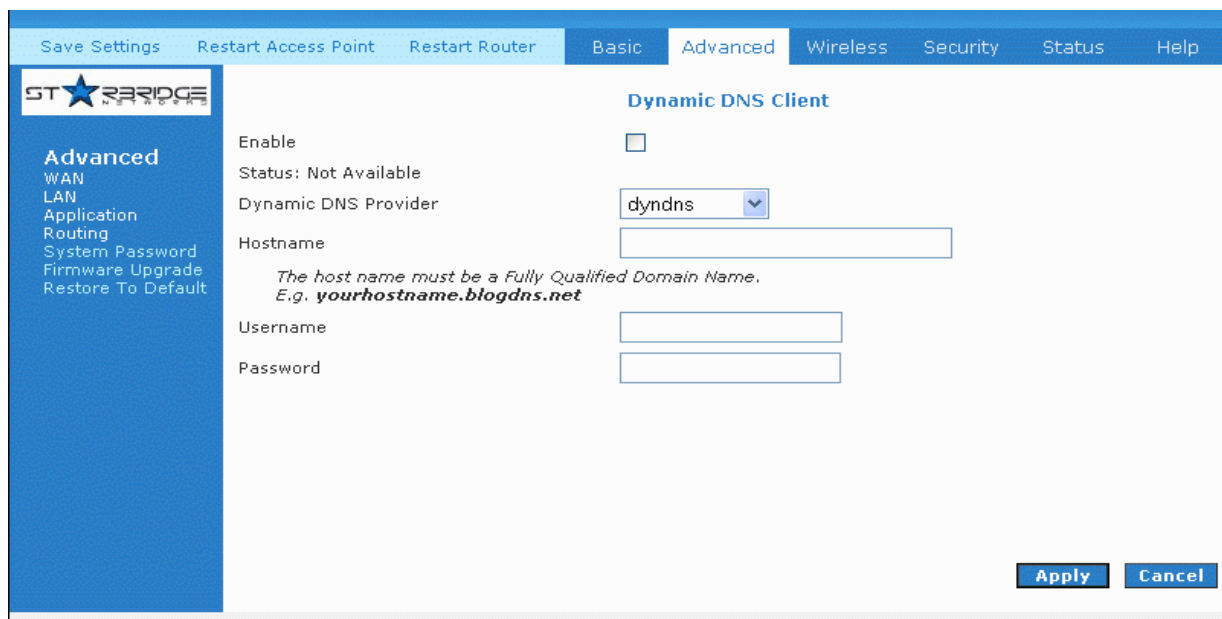


Figure 1-27: Dynamic DNS Client

6.3.14 DNS Proxy

This feature allows the user to select the (Domain Name Server) DNS Server Priority as well as enter IP addresses for Primary DNS and Secondary DNS. See Fig 1-28.

Save Settings Restart Access Point Restart Router Basic **Advanced** Wireless Security Status Help

STARRIDGE NETWORKS

Advanced
WAN
LAN
Application
Routing
System Password
Firmware Upgrade
Restore To Default

DNS Proxy

DNS Server Priority: Only Auto Discovered DNS Servers ▼

User Configured DNS Servers

Primary DNS:

Secondary DNS:

Apply Cancel

Figure 1-28: DNS Proxy

6.3.15 Easy Connect Configuration

Easy Connect feature allow user to surf web with ease without the need to changes default configuration setting, ie TCP/IP, Proxy, DNS of user's PC. See Fig 1-29.

There are 4 features on Easy Connect:

1. Auto IP: All valid TCP/IP setting on user's PC can surf web via ADSL modem routers without the need to change the IP address to the same subnet as the router or set to "Obtain an IP address automatically".
2. Auto DNS: Any DNS IP address set at user's PC irregardless whether the address is valid or invalid DNS, Auto DNS still allow user's PC to surf the web.
3. Auto Proxy: Any valid Private IP proxy setting with any port number, ie 1234 on the web browser such as Internet Explorer, Auto Proxy still allow PC to surf the web. Any Public IP proxy setting will assume the proxy is valid and hence Auto Proxy function will not take place.

Note: The port number to be used must be specify in both the web browser and the Auto Proxy Ports.

Private IP Ranges

Class A: 10.0.0.0 ~ 10.255.255.255

Class B: 172.16.0.0 ~ 172.31.255.255

Class C: 192.168.0.0 ~ 192.168.255.255

4. Auto NetBIOS: It allow proxy server to use any NetBIOS name which the Auto NetBIOS still allow PC to surf the web with a condition that the router gateway MUST be inPrivate IP Ranges.

The screenshot displays the 'Easy Connect Configuration' page in the StarBridge web interface. The top navigation bar includes 'Save Settings', 'Restart Access Point', 'Restart Router', 'Basic', 'Advanced' (selected), 'Wireless', 'Security', 'Status', and 'Help'. The left sidebar shows 'Advanced' selected, with sub-options: WAN, LAN, Application, Routing, System Password, Firmware Upgrade, and Restore To Default. The main content area is titled 'Easy Connect Configuration' and includes the instruction: 'To configure easy connect to allow user to access Internet without changes to PC Network Settings.' Below this, there is an 'Enable Easy Connect' checkbox (unchecked). The 'Feature Configuration' section shows four checked checkboxes: 'Auto IP', 'Auto DNS', 'Auto NETBIOS', and 'Auto Proxy'. The 'Proxy Ports' section contains four input fields with the values 8008, 8080, 8888, and 8000. At the bottom right, there are 'Apply' and 'Cancel' buttons.

Figure 1-29 : Easy Connect Configuration

6.3.16 Port Forwarding

Using the Port Forwarding page, you can provide local services (for example web hosting) for people on the Internet or play Internet games. When users send this type of request to your network via the Internet, the Lynx L-510 will forward those requests to the appropriate PC. Port forwarding can be used with DHCP assigned addresses but remember that a DHCP address is dynamic (not static). For example, if you were configuring a Netmeeting server, you would want to assign this server a static IP address so that the

IP address is not reassigned. Also remember that if an Internet user is trying to access an Internet application, they must use the WAN IP address. The port forwarding will translate the WAN IP address into a LAN IP address.

To configure a service, game, or other application select the external connection (for example the Internet connection), from the Home screen, click Advanced and under Advanced, select Port Forwarding. Next select the computer hosting the service and add the corresponding firewall rule. If you want to add a custom application, select the User category, click New and fill in the port, protocols and description for your application.

For example, if you want to host a Netmeeting session, from the Home screen, click Advanced and under Advanced, select Port Forwarding. First select the IP address for your Netmeeting server. Next select the Audio/Video category and add Netmeeting to the applied rules box. To view the management rules, highlight Netmeeting and select view; this will display the pre configured protocols and ports that Netmeeting will use. Now assuming that your WAN connection is correct, you can run Netmeeting from your server and call users that are on the Internet. If you know your WAN IP address, users can call you. See **Fig 1-30**.

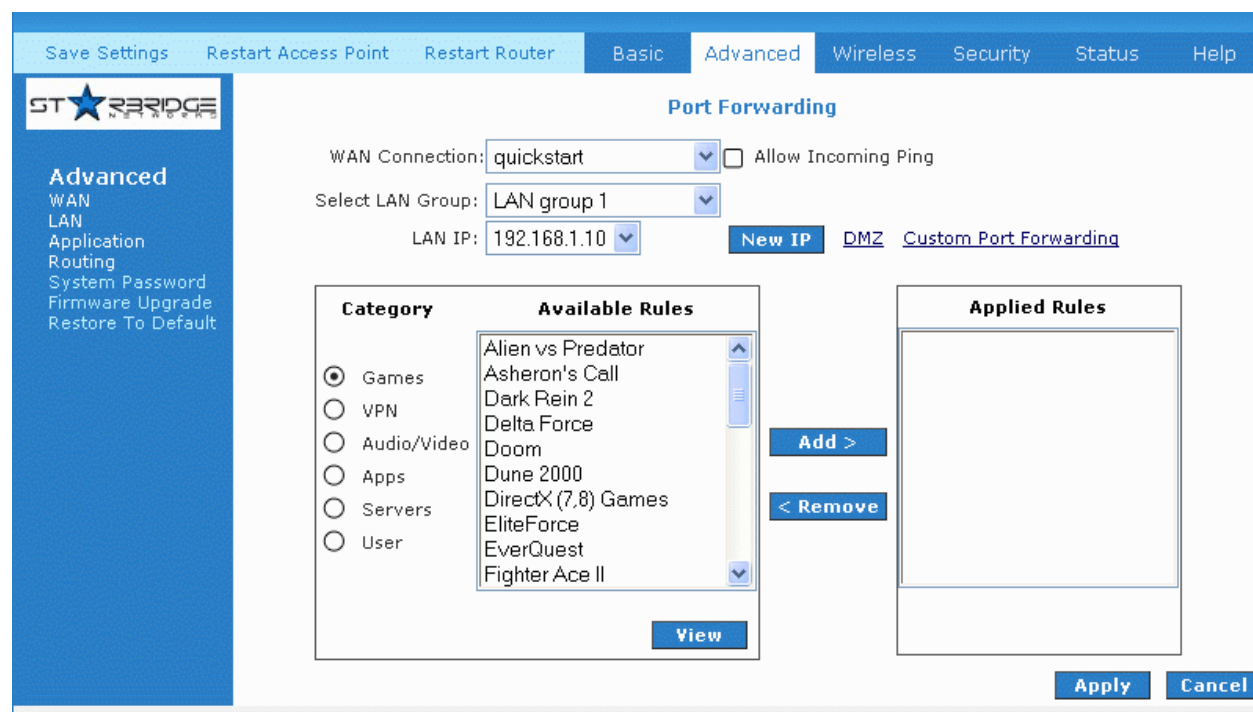


Figure 1-30: Port Forwarding

6.3.17 MAC Filtering (Bridge Filters)

The bridge filtering mechanism provides a way for the users to define rules to allow/deny frames through the bridge based on source MAC address, destination MAC address and/or frame type. When bridge filtering is enabled, each frame is examined against the each defined filter rules sequentially. When a matched is determined, the appropriate filtering action (determined by the access type selected ... i.e. allow or deny) is performed. Please note that the bridge filter will only examine frames from interfaces, which are part of the bridge itself. Twenty filter rules are supported with bridge filtering. See **Fig 1-31**.

Save Settings Restart Access Point Restart Router Basic **Advanced** Wireless Security Status Help

STARRIDGE

MAC Filtering

☐ Enable Bridge Filters
☐ Enable Bridge Filter Management Interface

Select LAN: LAN group 1

Bridge Filter Management Interface: USB

Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode
00-00-00-00-00-00	ANY	00-00-00-00-00-00	ANY	PPPoE Session	Deny

Add

Edit	Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode	Delete
------	---------	----------	----------	-----------	----------	------	--------

Apply Cancel

Figure 1-31: MAC Filtering (Bridge Filters)

6.3.18 Access Control

Access control allows you to open the access from the Internet LAN to the following management ports of the DSL600EU:

- Telnet
- Web
- FTP
- TFTP
- Secure Shell (SSH)
- SNMP

Fig 1-32 shows the default Access Control screen. The Access Control is disabled by default, remote management from the WAN side IP addresses is

denied, most services from the LAN side IP addresses is enabled. Remember to:

1. Check **Enable Access Control** to enable this feature. (This will enable the IP Access List field)
2. You can select an IP from the IP Access List, or enter a new IP and check **ADD**
3. Change the LAN and / or WAN configurations of the IP address
4. Click **Apply**

The screenshot shows the 'Access Control' configuration page of a STARRIDGE network device. The interface has a blue header with navigation tabs: 'Save Settings', 'Restart Access Point', 'Restart Router', 'Basic', 'Advanced' (selected), 'Wireless', 'Security', 'Status', and 'Help'. On the left, a sidebar lists 'Advanced' settings: WAN, LAN, Application, Routing, System Password, Firmware Upgrade, and Restore To Default. The main content area is titled 'Access Control' and contains the following elements:

- An unchecked checkbox for 'Enable Access Control'.
- A status message: 'All LAN access allowed, all WAN access denied.'
- A table with three columns: 'Service Name', 'WAN', and 'LAN group 1'.

Service Name	WAN	LAN group 1
Telnet	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Web	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FTP	<input type="checkbox"/>	<input checked="" type="checkbox"/>
TFTP	<input type="checkbox"/>	<input type="checkbox"/>
Secure Shell (SSH)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SNMP	<input type="checkbox"/>	<input type="checkbox"/>
- An 'IP Access List' section with a 'Select IP' dropdown menu, a 'Delete' checkbox, and a 'New IP' text input field with an 'Add' checkbox.
- 'Apply' and 'Cancel' buttons at the bottom right.

Figure 1-32: Access Control

6.3.19 Routing (Static Routing)

If the Lynx L-510 is connected to more than one network, you may need to set up a static route between them. A static route is a pre-defined pathway that network information must travel to reach a specific host or network. You can use static routing to allow different IP domain users to access the Internet through the Lynx L-510.

The New Destination IP is the address of the remote LAN network or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route here. For a standard Class C IP domain, the network address is the first three fields of the New Destination

IP, while the last field should be 0. The Subnet Mask identifies which portion of an IP address is the network portion, and which portion is the host portion. For a full Class C Subnet, the Subnet Mask is 255.255.255.0. The Gateway IP address should be the IP address of the gateway device that allows for contact between the Gateway and the remote network or host. The Hop Count determines the maximum number of steps between network nodes that data packets will travel. A node is any device on the network (such as a router or switch). See **Fig 1-33**.

The screenshot shows the 'Static Routing' configuration page in the StarLine Networks web interface. The 'Advanced' tab is selected, and the 'Static Routing' sub-tab is highlighted with a red circle. The page includes a left sidebar with navigation links: WAN, LAN, Application, Routing, System Password, Firmware Upgrade, and Restore To Default. The main content area has a 'Choose a connection:' dropdown menu set to 'quickstart'. Below this are input fields for 'New Destination IP:', 'Mask:' (pre-filled with '255.255.255.0'), 'Gateway:', and 'Metric:' (pre-filled with '0'). A message states 'The Routing Table is empty.' At the bottom right are 'Apply' and 'Cancel' buttons.

Figure 1-33: Static Routing

6.3.20 Dynamic Routing

Dynamic Routing allows the Lynx L-510 to automatically adjust to physical changes in the network. The Lynx L-510, using the RIP protocol, determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other Lynx L-510s on the network. The Direction determines the direction that RIP routes will be updated. Selecting In means that the Lynx L-510 will only incorporate received RIP information. Selecting Out means that the Lynx L-510 will only send out RIP information. Selecting both means that the Lynx L-510 will incorporate received RIP information and send out updated RIP information.

The protocol is dependent upon the entire network. Most networks support

Rip v1. If RIP v1 is selected, routing data will be sent in RIP v1 format. If Rip V2 is selected, routing data will be sent in RIP v2 format using subnet broadcasting. If Rip V1 Compatible is selected, routing data will be sent in RIP v2 format using multicasting. See **Fig 1-34**.

The screenshot shows the 'Dynamic Routing' configuration page in the STARRIDGE router web interface. The 'Advanced' tab is selected, and the 'Dynamic Routing' section is highlighted with a red circle. The page includes a sidebar with navigation links: Advanced, WAN, LAN, Application, Routing, System Password, Firmware Upgrade, and Restore To Default. The main content area contains the following settings:

- ☐ Enable RIP
- Protocol:
- ☒ Enable Password
- Password:
- Interface: LAN group 1, quickstart
- Direction: Both (dropdown), None (dropdown)

At the bottom right, there are 'Apply' and 'Cancel' buttons.

Figure 1-34: Dynamic Routing

6.3.21 System Password

You can change your Lynx L-510's username and password by clicking on User Management. From here you can change the login name and password. You can also change the idle timeout; you will need to log back onto the Lynx L-510 once the timeout expires. If you forget your password, you can press and hold the reset to factory defaults button for 10 seconds (or more). The Lynx L-510 will reset to its factory default configuration and all custom configurations will be lost.

The screenshot shows the 'System Password' configuration page in the STARRIDGE router web interface. The 'Advanced' tab is selected, and the 'System Password' section is highlighted with a red circle. The page includes a sidebar with navigation links: Advanced, WAN, LAN, Application, Routing, System Password, Firmware Upgrade, and Restore To Default. The main content area contains the following settings:

- System Password is used to change your User Name or Password.
- Enable Authentication: ☒
- User Name:
- Password:
- Confirmed Password:
- Idle Timeout: minutes

At the bottom right, there are 'Apply' and 'Cancel' buttons.

Figure 1-35: System Password

6.3.22 Firmware Upgrade

You can upgrade the Lynx L-510's firmware, clicking on Update Gateway under the Tools page. To upgrade the firmware, click browse, find the firmware file to download. Make sure this is the correct file. Click on upgrade firmware. Once the upgrade is complete the Lynx L-510 will reboot. You will need to log back onto the Lynx L-510 after the firmware upgrade is completed. The firmware upgrade should take about 5 minutes to complete. Note: Do not remove power from the Lynx L-510 during the firmware upgrade procedure.

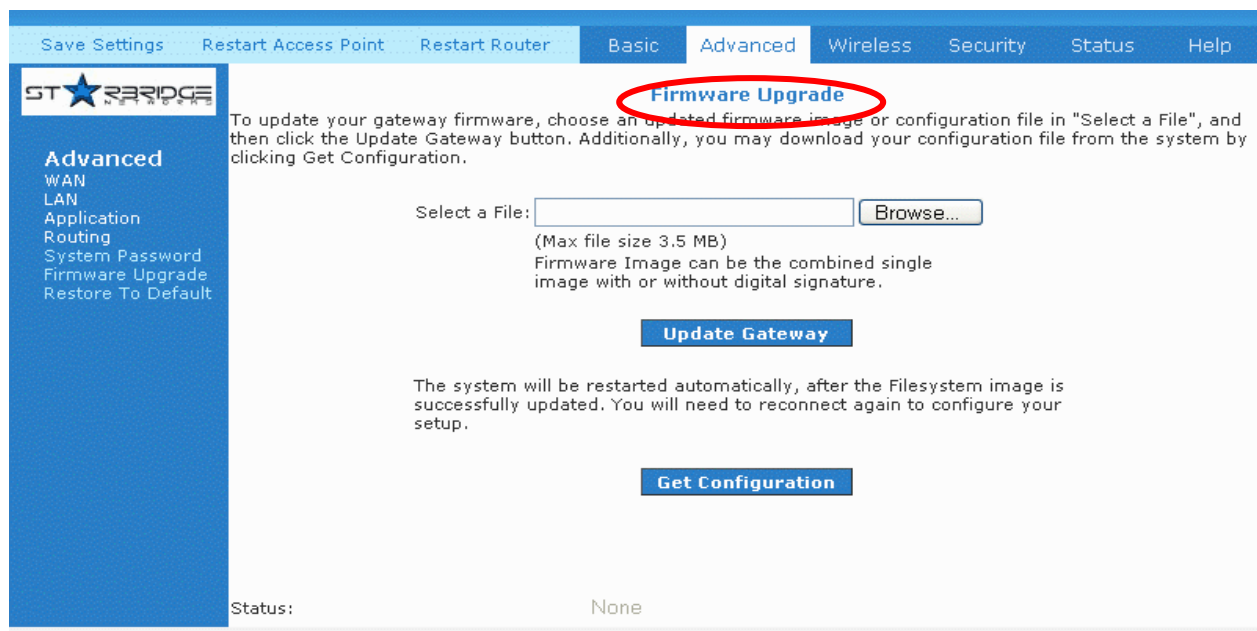


Figure 1-36: Firmware Upgrade

6.3.23 Restore to Default

The restore to factory defaults feature will set the Lynx L-510 to its factory default configuration by resetting the Lynx L-510. You may need to place the Lynx L-510 into its factory defaults if the configuration is changed, you lose the ability to interface to the Lynx L-510 via the web interface, or following a software upgrade. To reset the Lynx L-510, simply press the reset button for about ~ 10 seconds. The Lynx L-510 will be reset to its factory defaults and after about 30 ~ 40 seconds the Lynx L-510 will become operational again.

A prompt as the one shown in **Fig 1-37** will pop-up.

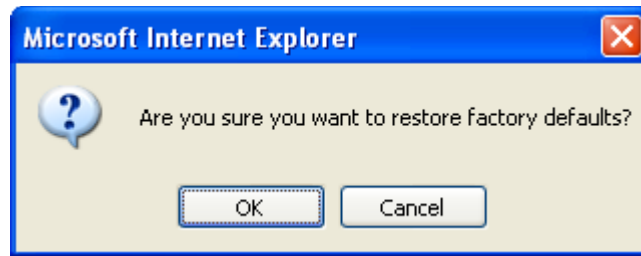


Figure 1-38: Restore to Default prompt

6.4 Wireless

6.4.1 Wireless Setup

The SSID default which is set as “yournetworkname” by default. It can be changed. SSID is wireless network name for the wireless router. Your wireless client will need this name for wireless connection. The wireless setup allows the user to enable or disable the AP (access point for the wireless feature). Disabling of A.P will prevent the wireless router from emitting any wireless signal. User can make change to the Country selection, which is set to default as Singapore. **See Fig 1-39.**

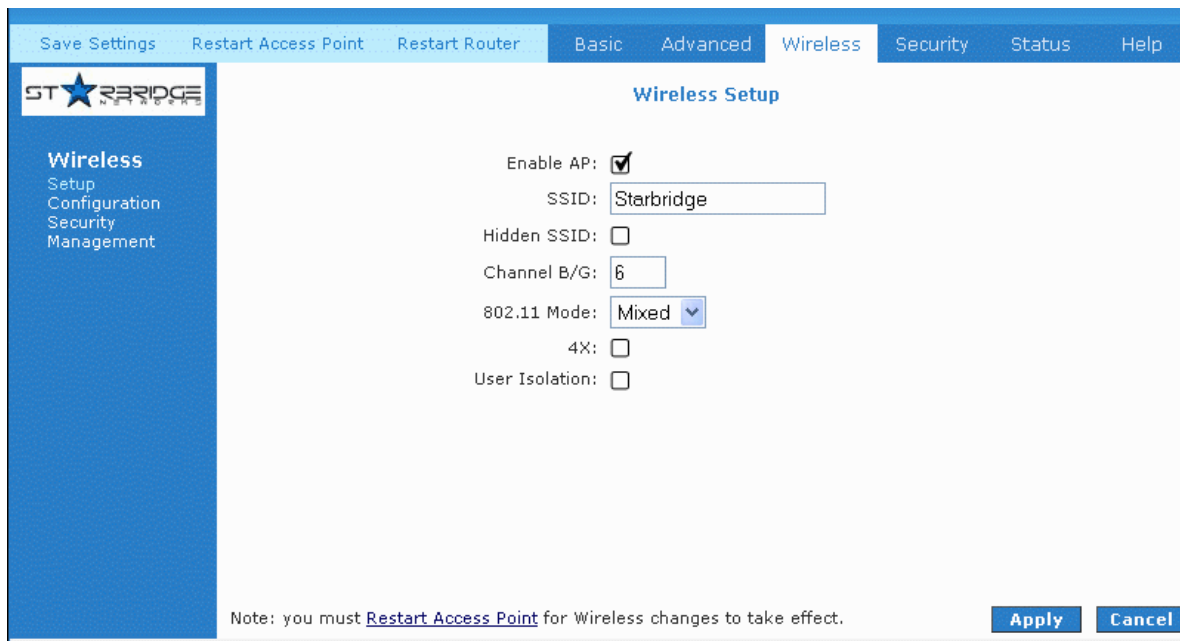
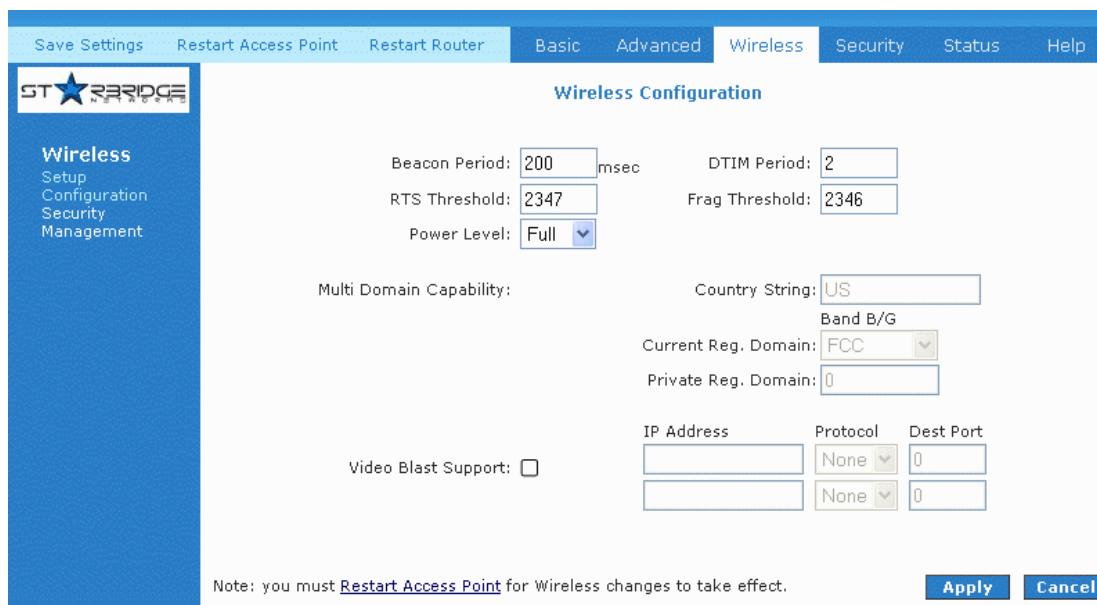


Figure 1-39: Wireless Setup Page

6.4.2 Wireless Configuration

For users who want to explore the advanced features, you can click on the Advanced button. The options listed can be changed to cater for advance users. **See Fig 1-40.**



The screenshot shows the 'Wireless Configuration' page of a StarBridge router. The top navigation bar includes 'Save Settings', 'Restart Access Point', 'Restart Router', 'Basic', 'Advanced', 'Wireless' (selected), 'Security', 'Status', and 'Help'. The left sidebar lists 'Wireless', 'Setup', 'Configuration', 'Security', and 'Management'. The main content area is titled 'Wireless Configuration' and contains the following fields:

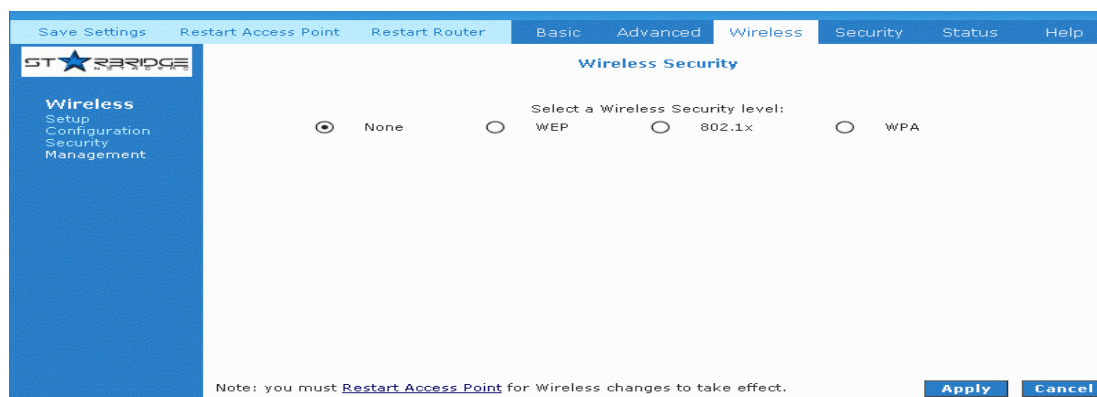
- Beacon Period: 200 msec
- DTIM Period: 2
- RTS Threshold: 2347
- Frag Threshold: 2346
- Power Level: Full (dropdown)
- Multi Domain Capability: (checkbox)
- Country String: US
- Band B/G: (dropdown)
- Current Reg. Domain: FCC (dropdown)
- Private Reg. Domain: 0
- Video Blast Support: (checkbox)
- IP Address: (text input)
- Protocol: None (dropdown)
- Dest Port: 0

At the bottom, there is a note: 'Note: you must [Restart Access Point](#) for Wireless changes to take effect.' and two buttons: 'Apply' and 'Cancel'.

Figure 1-40 : Wireless Configuration Page

6.4.3 Wireless Security

It is important for user to enforce security in wireless LAN environment; this is to prevent unauthorized wireless users from accessing your router. By default, the 'None' radio button is selected. **See Fig 1-41.**



The screenshot shows the 'Wireless Security' page of a StarBridge router. The top navigation bar is the same as in Figure 1-40, with 'Wireless' selected. The left sidebar is also the same. The main content area is titled 'Wireless Security' and contains the following fields:

- Select a Wireless Security level: (radio buttons)
- None (selected)
- WEP
- 802.1x
- WPA

At the bottom, there is a note: 'Note: you must [Restart Access Point](#) for Wireless changes to take effect.' and two buttons: 'Apply' and 'Cancel'.

Figure 1-41: Wireless Security

In order to implement security, proceed with the following steps. **See Fig 1-42.**

1. Select the WEP option.
2. Check on "Enable WEP Wireless Security" option.
3. Select the "Cipher" option, the available options are 64 bits, 128 bits and 256 bits.
4. You can configure up to 4 sets of keys for your wireless client.

Save Settings Restart Access Point Restart Router Basic Advanced **Wireless** Security Status Help

Wireless Security

Select a Wireless Security level:

☐ None ☒ WEP ☐ 802.1x ☐ WPA

☒ Enable WEP Wireless Security

Authentication Type: Open

Select	Encryption Key	Cipher
<input checked="" type="radio"/>		64 bits
<input type="radio"/>		64 bits
<input type="radio"/>		64 bits
<input type="radio"/>		64 bits

Enter 10, 26, or 58 hexadecimal digits for 64, 128 or 256 bit Encryption Keys respectively. e.g., AA AA AA AA AA for a key length of 64 bits.

Note: you must [Restart Access Point](#) for Wireless changes to take effect.

Apply Cancel

Figure 1-42: Wireless Security settings

Enter the IP Address of the RADIUS Server (for 802.1x authentication purposes). This is used only when you have a RADIUS Server and want to use it for authentication. Almost all homes and offices do not have a RADIUS Server.

Save Settings Restart Access Point Restart Router Basic Advanced **Wireless** Security Status Help

STARRIDGE

Wireless
Setup
Configuration
Security
Management

Select a Wireless Security level:

☐ None ☐ WEP ☒ 802.1x ☐ WPA

Radius Settings

Server IP Address:

Port:

Secret:

Group Key Interval:

Note: you must [Restart Access Point](#) for Wireless changes to take effect.

Apply Cancel

Figure 1-43 : Wireless Security

WPA is the short term for WiFi Protected Access. WPA is an industry-supported, pre-standard version of 802.11i that utilizes the Temporal Key Integrity Protocol (TKIP), which fixes the problems of WEP, which includes using dynamic keys.

Save Settings Restart Access Point Restart Router Basic Advanced **Wireless** Security Status Help

STARRIDGE

Wireless
Setup
Configuration
Security
Management

Select a Wireless Security level:

☐ None ☐ WEP ☒ 802.1x ☐ WPA

Group Key Interval:

Note: Group Key Interval is shared by all WPA options.

☒ 802.1x Server IP Address:

Port:

Secret:

☐ PSK String String: (Max 63 characters)

Note: you must [Restart Access Point](#) for Wireless changes to take effect.

Apply Cancel

Figure 1-44 : Wireless Security

6.4.4 Wireless Management

Wireless Management consists of Access List, Associated Stations and Multiple SSID.

6.4.4.1 Access List

This feature permits you to "Allow" or "Ban" any wireless client from accessing the wireless router. You must add the MAC address of the client's wireless LAN card.

6.4.4.2 Associated Stations

Wireless client which are connected to the wireless router will be displayed in this screen. You are able to ban this station by clicking on the "Ban Station" option. Then click on "Apply" button.

6.4.4.3 Multiple SSID

This router supports multiple SSID, which means that you can set more than one SSID for this router.

Save Settings Restart Access Point Restart Router Basic Advanced **Wireless** Security Status Help

STARRIDGE NETWORKS

Wireless Management

Wireless
Setup
Configuration
Security
Management

Access List **Associated Stations** **Multiple SSID**

Access List

☐ Enable Access List

☐ Allow ☐ Ban

Mac Address: **Add**

Note: you must [Restart Access Point](#) for Wireless changes to take effect. **Apply** **Cancel**

Figure 1-45: Wireless Management

6.5 Security

The security feature section allows users to configure the following:

- IP Filters
- LAN Isolation
- URL Filters

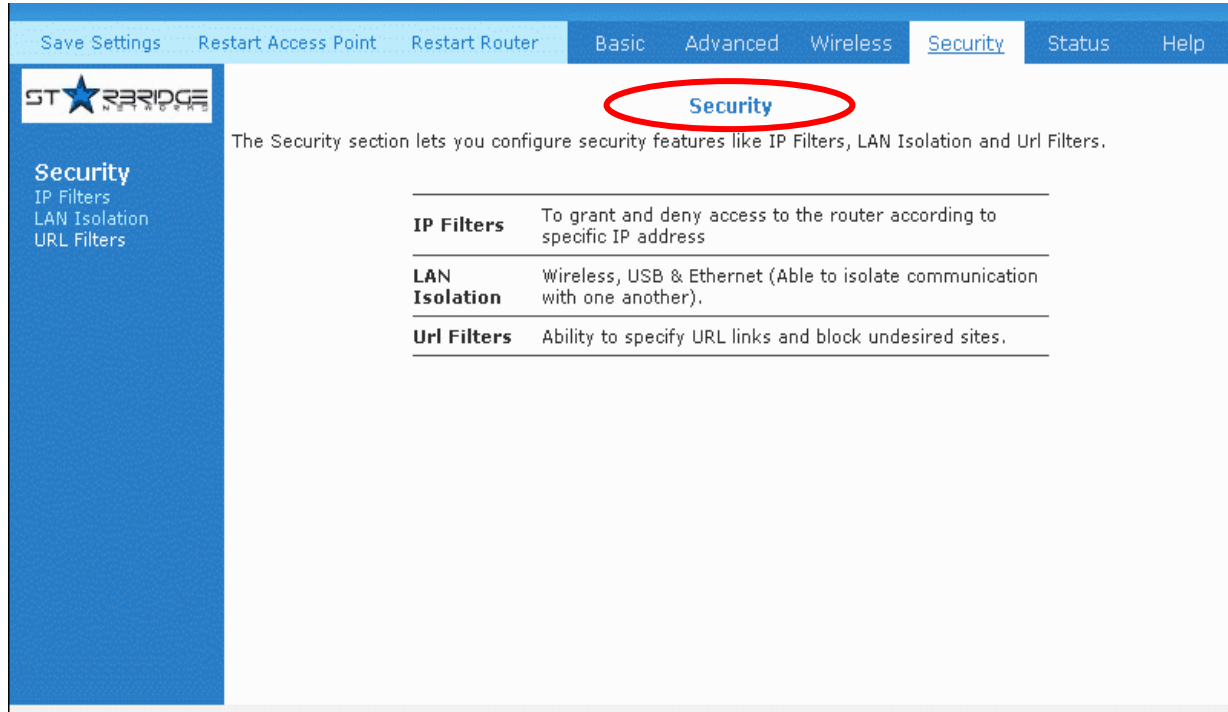


Figure 1-46: Security

6.5.1 IP Filters

IP filter is identical to what Port blocking to Access Control. **Fig 1-47** demonstrates that the router will block workstations with the IP in the defined range of 192.168.1.5 to 192.168.1.20 and port range from 2000 to 3000.

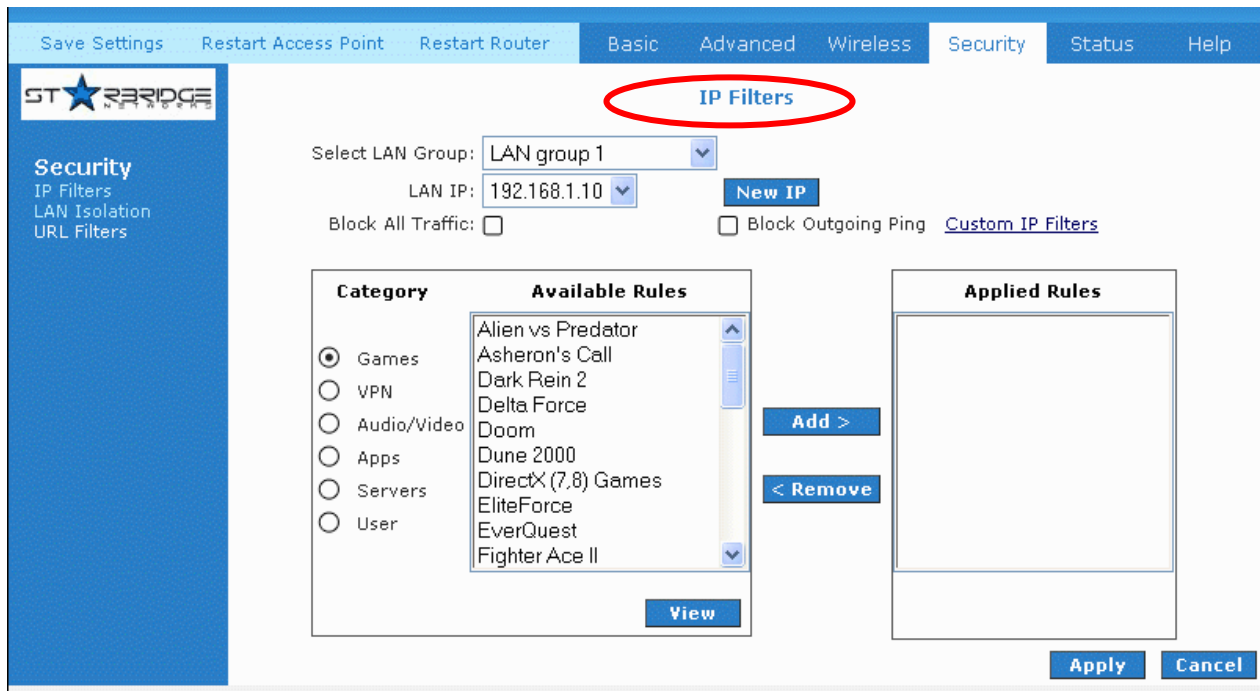


Figure 1-47: IP Filters

6.5.2 LAN Isolation

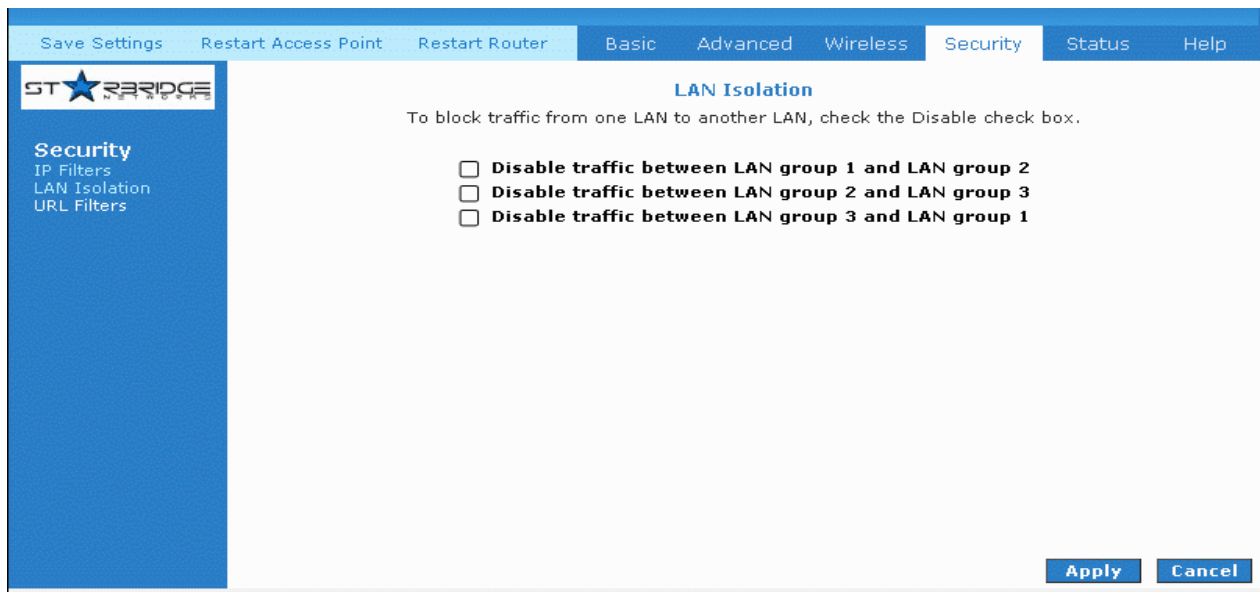


Figure 1-48: LAN Isolation

LAN isolation allows you to disable the flow of packets between up to three-user-defined LAN groups (WLAN, USB and Ethernet). This allows you to secure information in private portions of the LAN from other, publicly accessible LAN segments.

6.6 Status

This status section allows users to view the following connections and interfaces:

- Connection Status
- System Log
- Remote Log
- Network Statistics
- DHCP Clients
- Modem Status
- Product Information

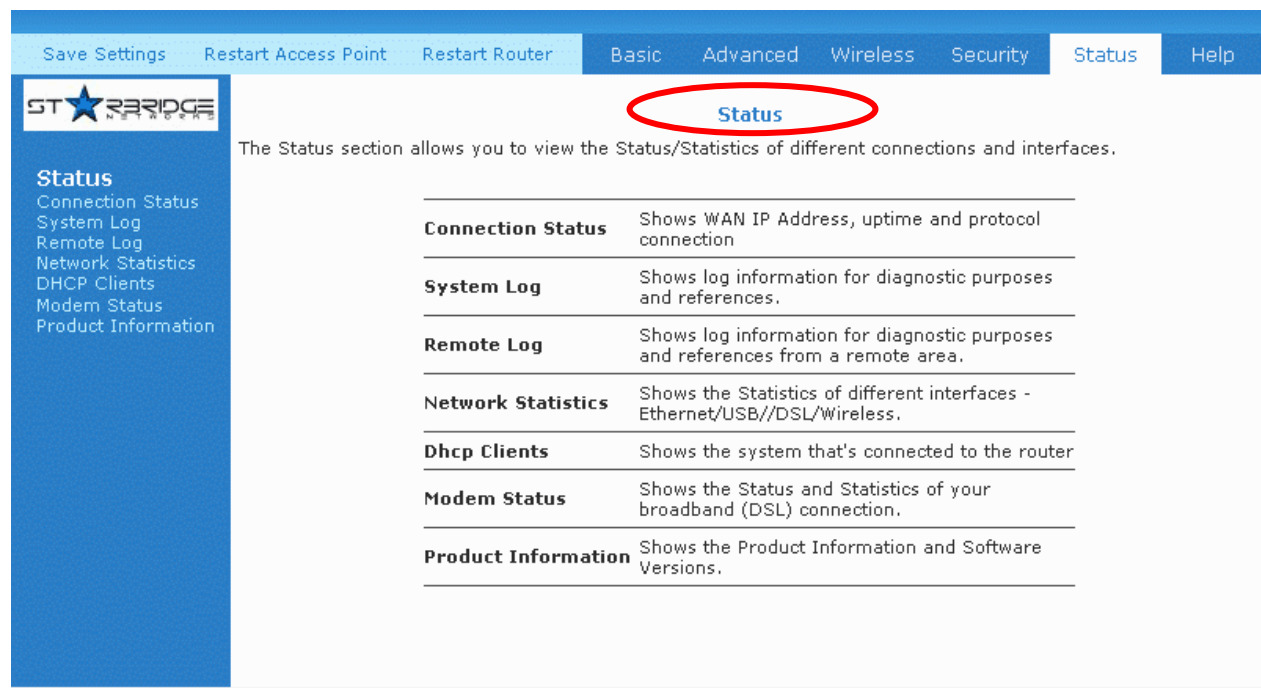


Figure 1-49: Status

6.6.1 Connection Status

Connection Status will display all the relevant information regarding your Internet Connection, it will display the type of protocol used, the WAN IP address, the connection state, the duration and if it is Disconnected the reason will be displayed. The "Disconnect" button on the right-hand side is

for terminating the connection from the Internet. See **Fig 1-50**



Figure 1-50: Connection Status

6.6.2 System Log

You can display the Lynx L-510's log by going under the Status title, click on System log. From here you can view all logged information. Depending upon the severity level, this logged info will generate log reports to a remote host (if remote logging is enabled).



Figure 1-51: System Log

6.6.3 Remote Log Settings

This feature is for users to enable remote logging. Settings mentioned below are essential for this feature to work:

- Log Level
- Adding / Deleting IP address
- Logging destination

The screenshot shows the 'Remote Log Settings' page. At the top, there is a navigation bar with tabs: 'Save Settings', 'Restart Access Point', 'Restart Router', 'Basic', 'Advanced', 'Wireless', 'Security', 'Status', and 'Help'. The 'Status' tab is selected. On the left, a sidebar menu lists: 'Status', 'Connection Status', 'System Log', 'Remote Log', 'Network Statistics', 'DHCP Clients', 'Modem Status', and 'Product Information'. The main content area is titled 'Remote Log Settings'. It contains a 'Log Level' section with a dropdown menu set to 'Notice'. Below this is an 'Add an IP Address' section with a text input field and an 'Add' button. Further down is a 'Select a logging destination' section with a dropdown menu set to 'None' and a 'Delete' button. At the bottom right, there are 'Apply' and 'Cancel' buttons.

Figure 1-52: Remote Log Settings

6.6.4 Network Statistics

Information regarding the Status and Statistics of your Ethernet, USB and DSL line will be displayed.

The screenshot shows the 'Network Statistics' page. At the top, there is a navigation bar with tabs: 'Save Settings', 'Restart Access Point', 'Restart Router', 'Basic', 'Advanced', 'Wireless', 'Security', 'Status', and 'Help'. The 'Status' tab is selected. On the left, a sidebar menu lists: 'Status', 'Connection Status', 'System Log', 'Remote Log', 'Network Statistics', 'DHCP Clients', 'Modem Status', and 'Product Information'. The main content area is titled 'Network Statistics'. It starts with the instruction 'Choose an interface to view your network statistics:'. Below this are four radio buttons: 'Ethernet' (selected), 'USB', 'DSL', and 'Wireless'. The statistics are divided into 'Transmit' and 'Receive' sections. The 'Transmit' section includes: 'Good Tx Frames' (5717), 'Good Tx Broadcast Frames' (278), 'Good Tx Multicast Frames' (45), 'Tx Total Bytes' (4623697), 'Collisions' (0), 'Error Frames' (0), and 'Carrier Sense Errors' (0). The 'Receive' section includes: 'Good Rx Frames' (3182), 'Good Rx Broadcast Frames' (86), 'Good Rx Multicast Frames' (15), 'Rx Total Bytes' (311039), 'CRC Errors' (0), 'Undersized Frames' (0), and 'Overruns' (0). At the bottom right, there is a 'Refresh' button.

Figure 1-53: Network Statistics

6.6.5 DHCP Clients

Shows the users connected. It also shows the MAC address, IP address, host name and lease time.

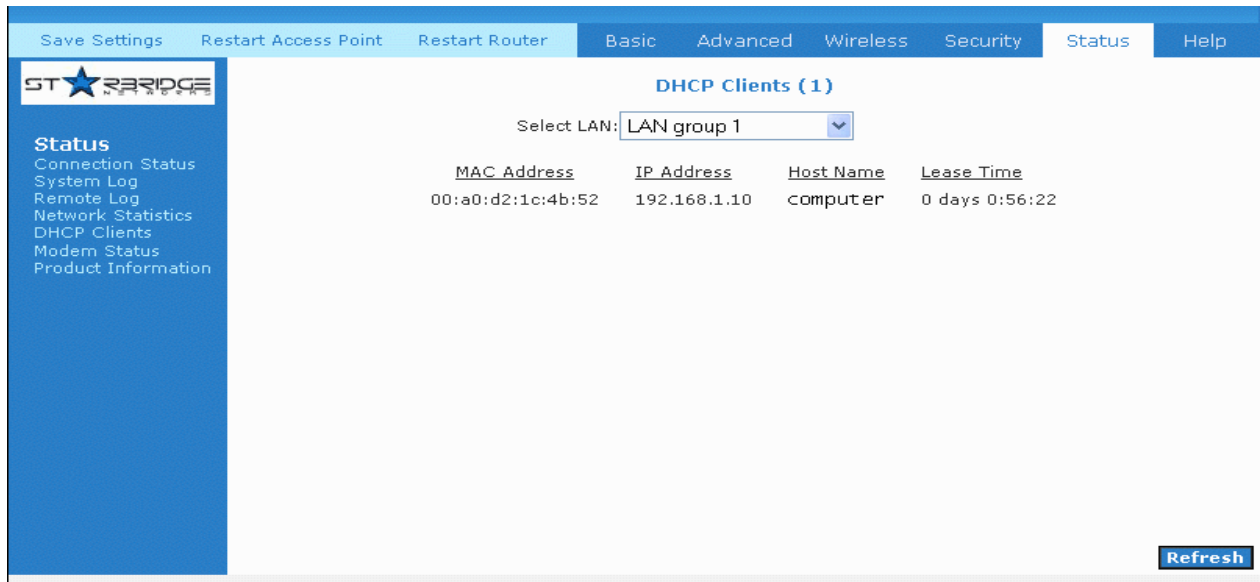


Figure 1-54: DHCP Clients

6.6.6 Modem Status

This screen will display the Modem status and DSL statistics.

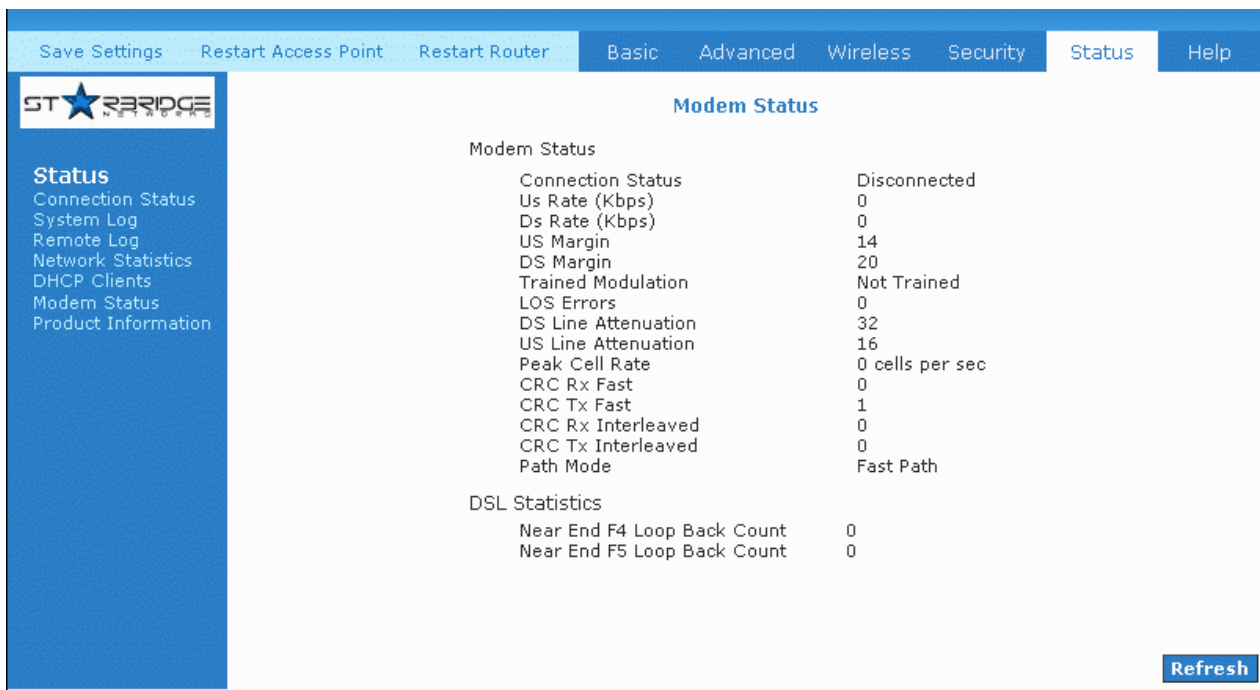


Figure 1-55: Modem Status

6.6.7 Product Information

This screen will show a summary of all the product information and software version that comes bundled with the Lynx L-510.

The screenshot shows the 'Product Information' page of the STARRIDGE router web interface. The top navigation bar includes 'Save Settings', 'Restart Access Point', 'Restart Router', 'Basic', 'Advanced', 'Wireless', 'Security', 'Status', and 'Help'. The left sidebar shows 'Status' as the active section, with sub-links for 'Connection Status', 'System Log', 'Remote Log', 'Network Statistics', 'DHCP Clients', 'Modem Status', and 'Product Information'. The main content area is titled 'Product Information' and contains two sections: 'Product Information' and 'Software Versions'.

Product Information	
Model Number	Lynx510
HW Revision	Unknown
Serial Number	none
USB PID	0x6060
USB VID	0x0451
Ethernet MAC	00:e0:a0:a6:66:70
DSL MAC	N/A
USB MAC	00:E0:A6:66:41:EB
USB Host MAC	00:E0:A6:66:41:E1
AP MAC	00:50:f1:12:12:10

Software Versions	
Gateway	3.6.0C
Firmware	73.48.2
ATM Driver	4.05.11.00
DSL HAL	4.01.00.05
DSL Datapump	4.01.02.00 Annex A
SAR HAL	01.07.2a
PDSP Firmware	0.50
Wireless Firmware	1.6.0.24
Wireless APDK	5.7.0.6
Boot Loader	0.22.03

Figure 1-56: Product Information

6.7 Help

The Help screen takes you to the different Help Sections for Firewall, Bridge Filters, LAN Clients, LAN Group Configurations, PPP Connection, UPnP, IP QoS and RIP Help.

The screenshot shows the 'Help' page of the STARRIDGE router web interface. The top navigation bar is the same as in Figure 1-56, with 'Help' now selected. The left sidebar remains the same. The main content area is titled 'Help' and contains a paragraph: 'This section takes you to different Help Sections for Firewall, Bridge Filters, LAN Clients, LAN Configuration, PPP Connection, UPnP, IPQos and RIP.' Below this is a table listing the help sections.

	Help
Firewall	Help for Port Forwarding, Access Control, and Advanced Security.
Bridge Filters	Help section for Bridge Filters.
LAN Clients	Help section for LAN Clients.
LAN Group Configuration	Help section for Configuring LAN Groups with static IP Address.
PPP Connection	Help for establishing a PPP Connection.
UPnP	Help pages for UPnP.
IP QoS	Help section for IP QoS.
RIP Help	Help section for RIP (Routing Information Protocol).

Figure 1-57: Help Screen

Appendix A: Troubleshooting

Below is a list of commonly asked questions. Before calling technical support, please look through these issues to see if they help to solve your problem.

The Lynx L-510 is not working

1. Check to see that the power LED is green and that the network cables are installed correctly. Refer to the easy start guide for more details.
2. Check to see that the ETH/LAN and PPP/WAN LEDs are green.
3. Check to see that the DSL LED is green
4. Make sure you are not connecting the USB and the Ethernet port at the same time. You must only use 1 interface at a time.
5. Check the settings on your PC. Again, refer to the easy start guide for more details
6. Check the Lynx L-510's settings.
7. From your PC, can you PING the Lynx L-510? Assuming that the Lynx L-510 has DHCP enabled and your PC is on the same subnet as the gateway, you should be able to PING the gateway.
8. Can you PING the WAN IP? Your ISP should have provided the IP address of their server. If you can ping the Lynx L-510 and your protocols are configured correctly, you should be able to ping the ISPs network. If you cannot PING the ISPs network, make sure you are using the correct protocols with the correct VPI/VCI values.
9. Make sure NAT is enabled for your connection. If NAT is disabled the Lynx L-510 will not route frames correctly (except in Bridge connection).

I can't connect to the Lynx L-510

1. Check to see that the power LED is green and that the network cables are installed correctly; see the easy start guide for more details.
2. Make sure you are not connecting the USB and the Ethernet port at the same time. You must only use 1 interface at a time.
3. Make sure that your PC and the Lynx L-510 is on the same network segment. The Lynx L-510's default IP address is 192.168.1.1. If you are running a Windows based PC, you can open a DOS window and type IPCONFIG; make sure that the network adapter that is connected to the gateway is within the same 192.168.1.x subnet.
4. Also, your PC's Subnet Mask should match the gateways subnet mask. The gateway has a default subnet mask of 255.255.255.0.

-
5. If this still does not work, press the reset button for 10 seconds. This will place the gateway into its factory default state. Go through the above procedures again.
 6. Make sure NAT is enabled for your connection. If NAT is disabled the Lynx L-510 will not route frames correctly (except in Bridge connection).

The DSL Link LED continues to blink but does not go solid

1. This means that the DSL line is trying to train but for some reason it cannot establish a valid connection. The main cause of this is that you are too far away from the central office. Contact your DSL service provider for further assistance.
2. Verify that the phone line is connected directly to the wall and to the line input on the Lynx L-510.
3. Make sure that for every parallel phone line connected to telephone or fax to install with a micro filter.

The DSL Link LED is always off

1. Make sure you have DSL service. You should get some kind of information from your ISP that states that DSL service is installed. You can usually tell if the service is installed by listening to the phone line; you will hear some high-pitched noise. If you do not hear high-pitched noise, contact your ISP.
2. Verify that the phone line is connected directly to the wall and to the line input on the Lynx L-510. If the phone line is connected to the phone side of the Lynx L-510 or you have a splitter installed on the phone line, the DSL light will not come on.

APPENDIX B: Lynx L-510 terms

What is a firewall?

A firewall is protection between the Internet and your local network. It acts similarly to the firewall in your car, protecting the interior of the car from the engine. Your car's firewall has very small opening that allow desired connections from the engine into the cabin (gas pedal connection, etc), but if something happens to your engine, you are protected.

The firewall in the Lynx L-510 is very similar. Only the desired connections that you allow are passed through the firewall. These connections are normally originating from the local network; such as web browsing, checking your email, downloading a file, and playing a game. However, in some cases, you can allow incoming connections so that you can run programs like a web server.

What is NAT?

NAT stands for Network Address Translation. Another name for it is Connection Sharing. What does this mean? Your ISP provides you with a single network address for you to access the Internet through. However, you may have several machines on your local network that want to access the Internet at the same time. The Lynx L-510 provides NAT functionality that converts your local network addresses to the single network address provided by your ISP. It keeps track of all these connections and makes sure that the correct information gets to the correct local machine. Occasionally, there are certain programs that don't work well through NAT. Some games, and some specialty applications have a bit of trouble. The Lynx L-510 contains special functionality to handle the vast majority of these troublesome programs and games. NAT does cause problems when you want to run a SERVER though. When running a server, please see the DMZ section below.

What is a DMZ?

DMZ really stands for Demilitarized Zone. It is a way of separating out part of your local network so that is more open to the Internet. Suppose that you want to run a web-server, or a game server. Normal servers like these are blocked from working by the NAT functionality. The solution is to "isolate"

the single local computer into a DMZ. This makes the single computer look like it is directly on the Internet, and others can access this machine.

Your machine isn't really directly connected to the Internet, and it really has an internal local network address. When you provide the servers network address to others, you must provide the address of the Lynx L-510. The Lynx L-510 "fakes" the connection to your machine.

You should use the DMZ when you want to run a server that others will access from the Internet. Internal programs and servers (like print servers, etc) should NOT be connected to the DMZ

What is a Gateway?

The Internet is so large that a single network cannot handle all of the traffic and still deliver a reasonable level of service. To overcome this limitation, the network is broken down into smaller segments or subnets that can deliver good performance for the stations attached to that segment. This segmentation solves the problem of supporting a large number of stations, but introduces the problem of getting traffic from one subnet to another.

To accomplish this, devices called routers or gateways are placed between segments. If a machine wishes to contact another device on the same segment, it transmits to that station directly using a simple discovery technique. If the target station does not exist on the same segment as the source station, then the source actually has no idea how to get to the target.

One of the configuration parameters transmitted to each network device is its default gateway. This address is configured by the network administrators and it informs each personal computer or other network device where to send data if the target station does not reside on the same subnet as the source. If your machine can reach all stations on the same subnet (usually a building or a sector within a building), but cannot communicate outside of this area, it is usually because of an incorrectly configured default gateway.



© 2005 Starbridge Networks LLC. All rights reserved.

www.starbridgenetworks.com



Lynx: constellation introduced by J. Hevelius in 1687. The Lynx is a nocturnal wildcat with superb eyesight. The observers of this constellation would have to be “lynx-eyed” to see it.